Stateless Approach to End-to-End Security for the Internet of Things

(OSCAR – Object Security Architecture for the IoT)

Mališa Vučinić ❖★, Bernard Tourancheau ❖, Franck Rousseau ❖, Andrzej Duda ❖, Laurent Damon ★, and Roberto Guizzetti ★.

❖ Grenoble Informatics Laboratory, France

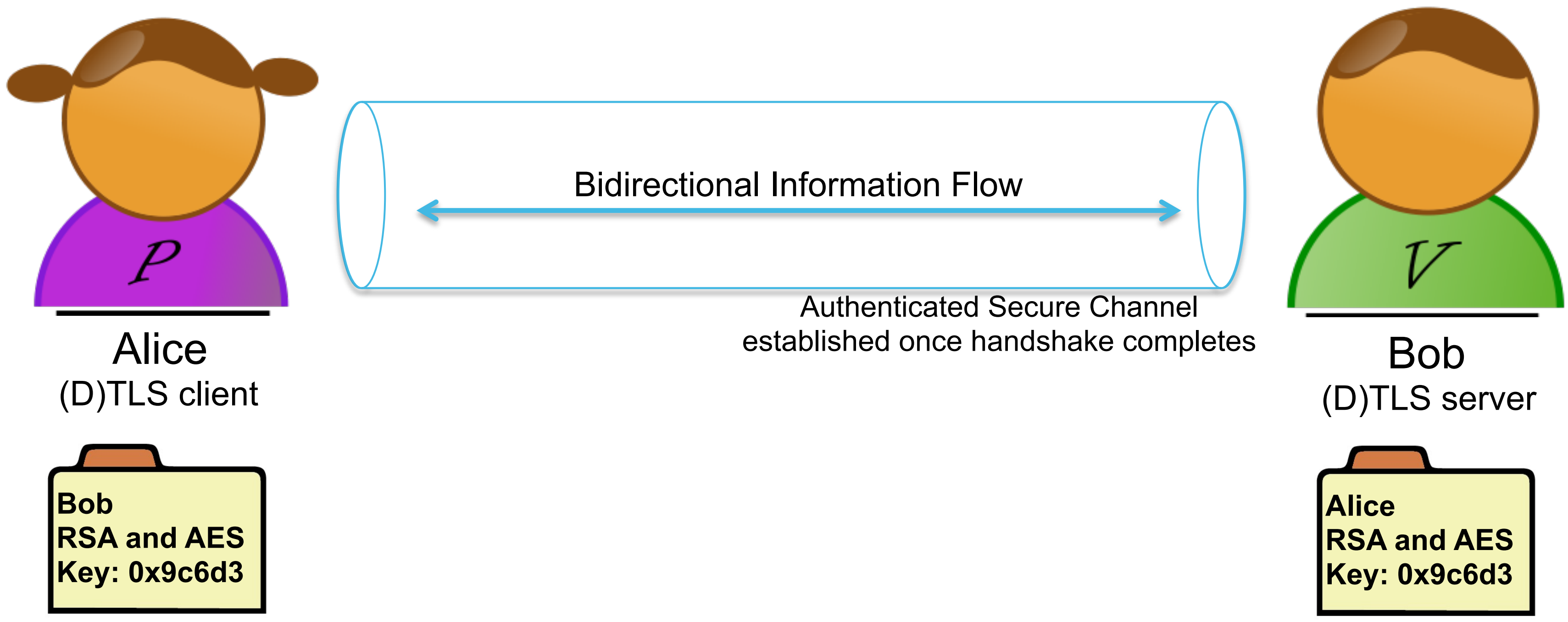
★ STMicroelectronics

Montbonnot, November 6th 2014

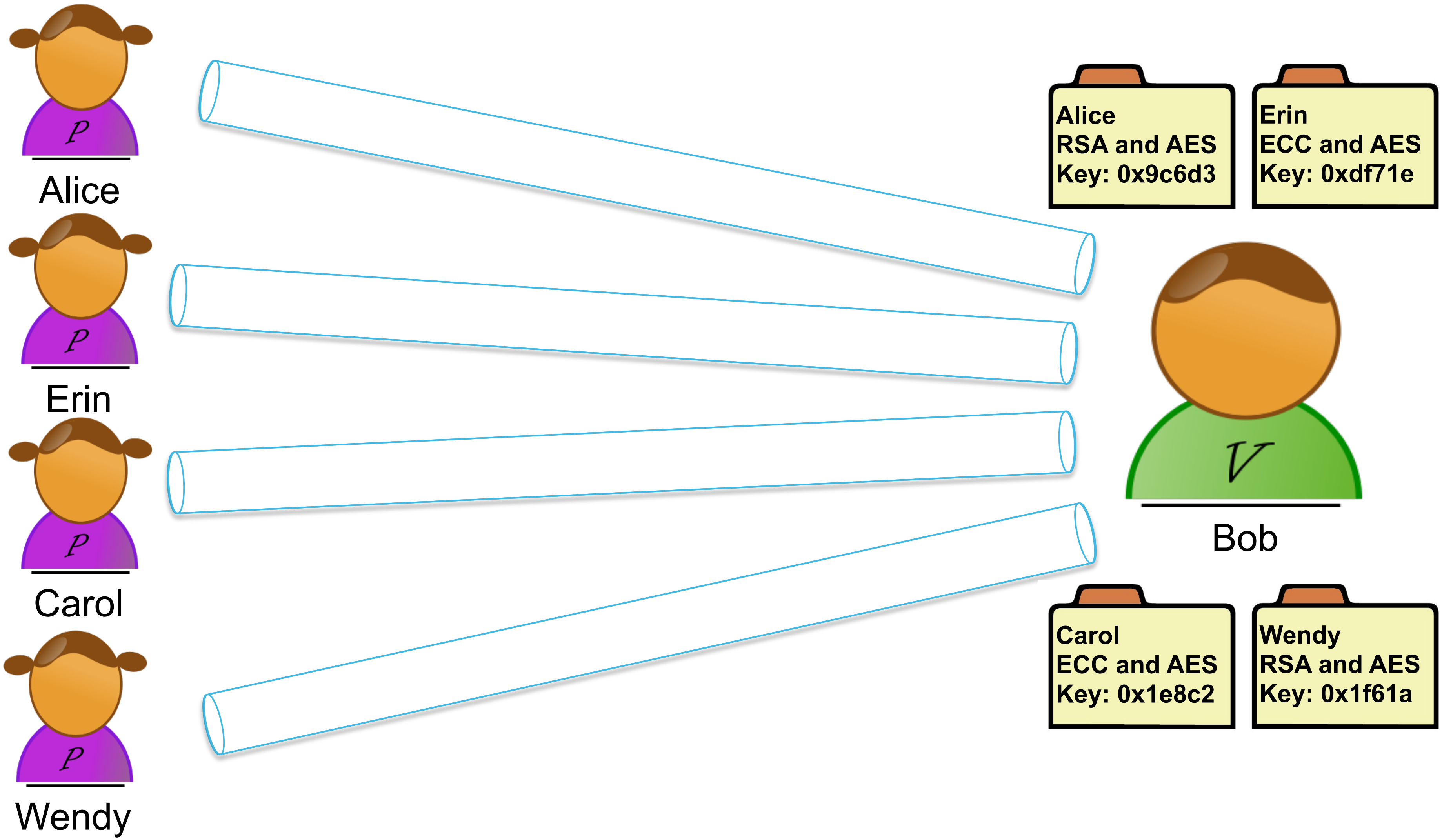
life.augmented

L I G

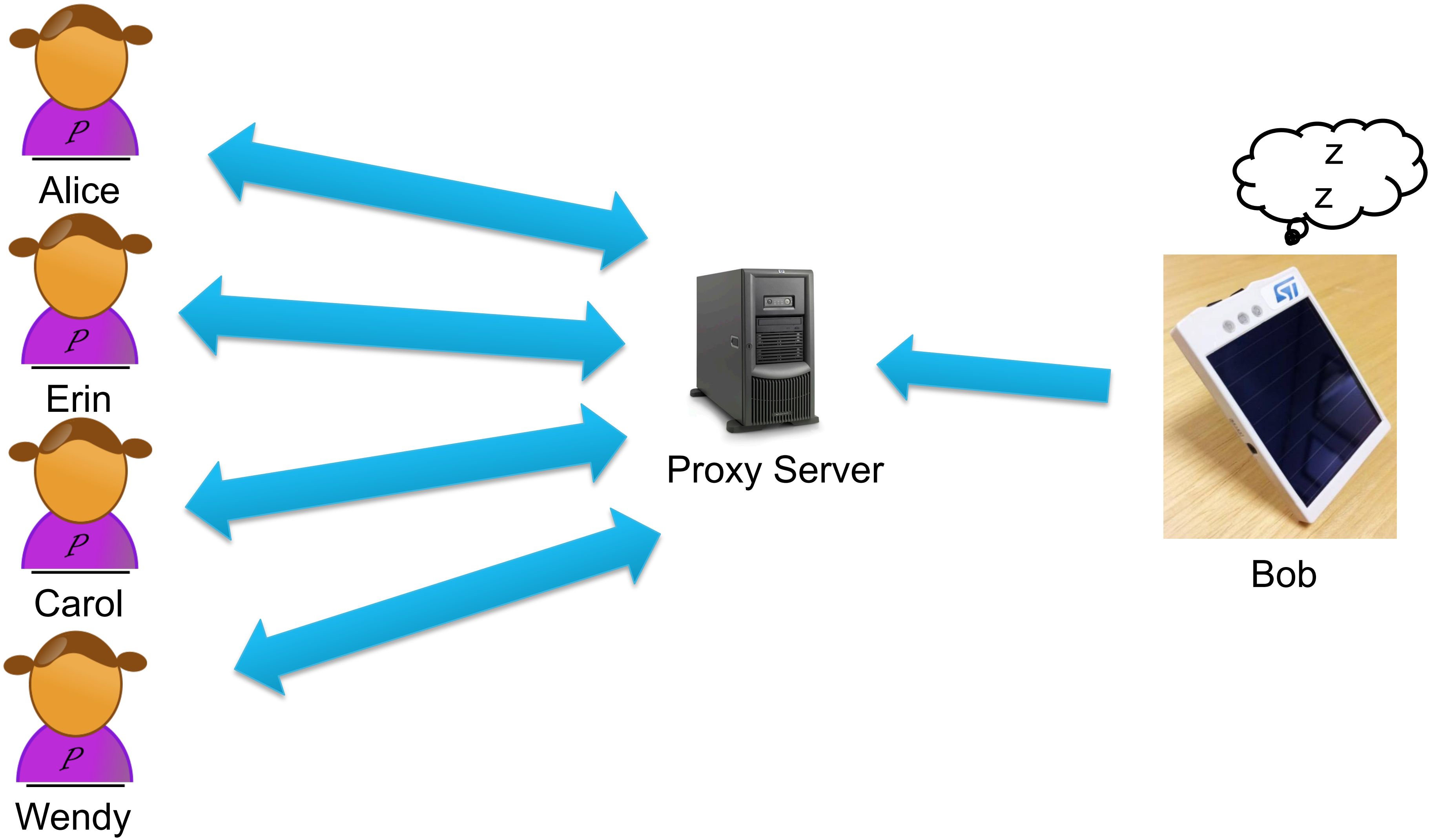
Security in the traditional Internet (1/2)



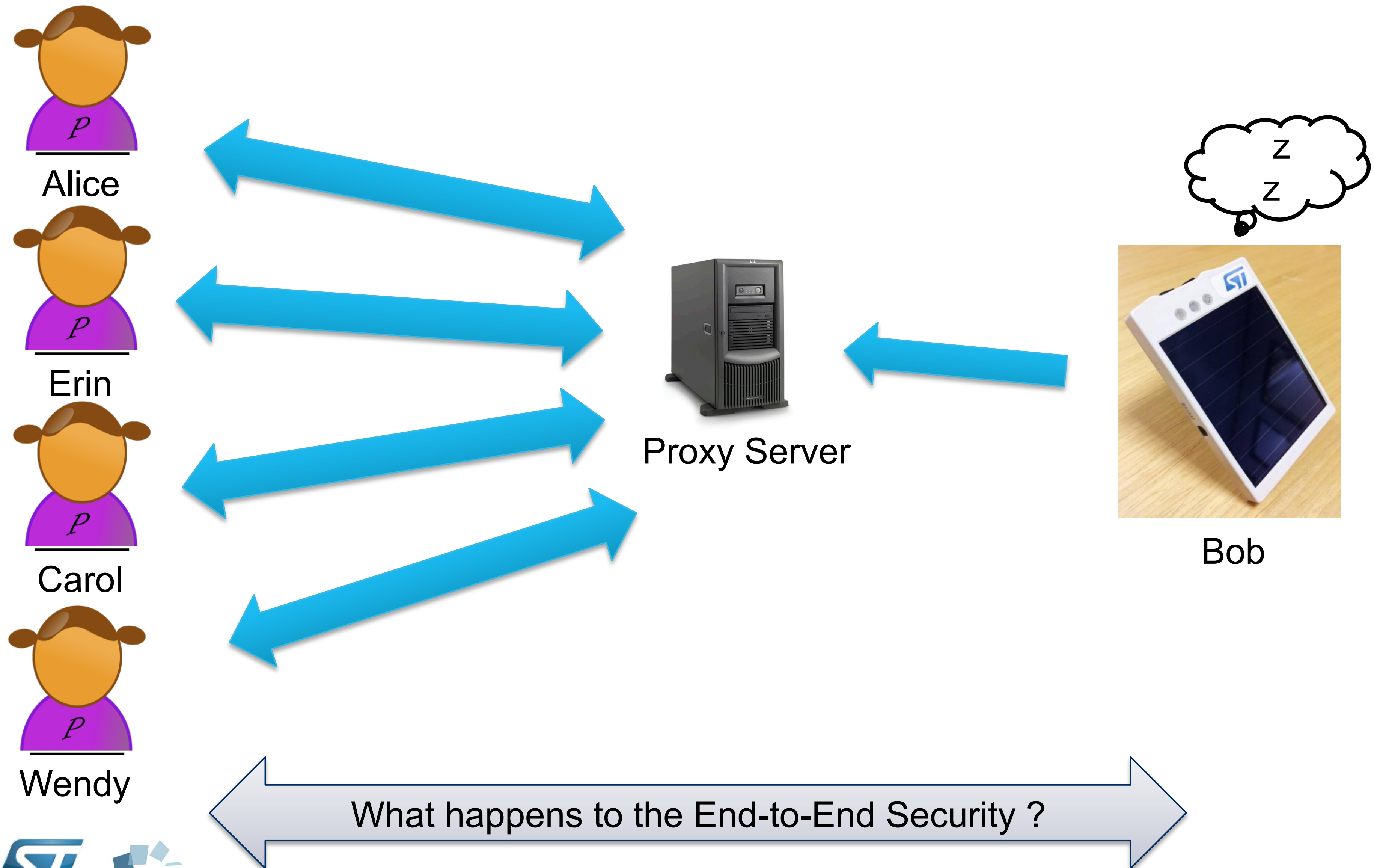
Security in the traditional Internet (2/2)



Security in the Internet of Things



Security in the Internet of Things



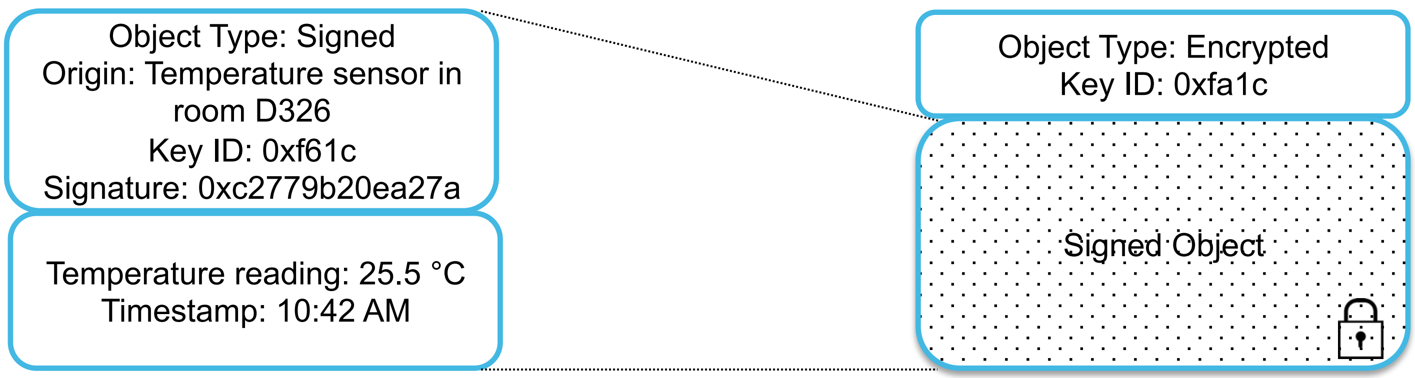
Motivation

- Features of the Constrained Application Protocol (CoAP) when secured by DTLS:
  - Group communication i.e. multicast support ✗
  - Asynchronous message exchanges ±
  - Proxy and caching capabilities ✗
  - Low overhead ✗
  - Header mapping to HTTP ✗

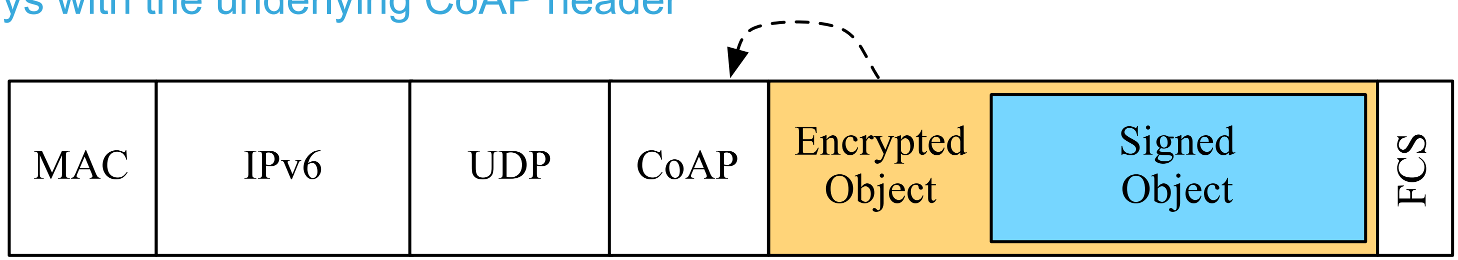
OSCAR – concepts behind (1/2)

Object Security Architecture for the Internet of Things [1]

- **Idea 1:** A stateless security architecture
  - Allows caching, eases group communication and asynchronous exchanges
  - Solution: Object security – Application data encapsulated within “secured objects”



  - Protect from communication-related attacks by binding object-security encryption keys with the underlying CoAP header



[1] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, R. Guizzetti,
OSCAR: Object Security Architecture for the Internet of Things, in: WoWMoM, IEEE, 2014, pp. 1–10.

OSCAR – concepts behind (2/2)

Object Security Architecture for the Internet of Things [1]

- **Idea 2:** Move the burden of security handshake away from sensors
  - Introduce a **semi**-trusted, non-constrained third party that will do the hard work
  - Sensors respond with secured objects (resource representations) regardless of the identity of the client

[1] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, R. Guizzetti,
OSCAR: Object Security Architecture for the Internet of Things, in: WoWMoM, IEEE, 2014, pp. 1–10.

OSCAR – concepts behind (2/2)

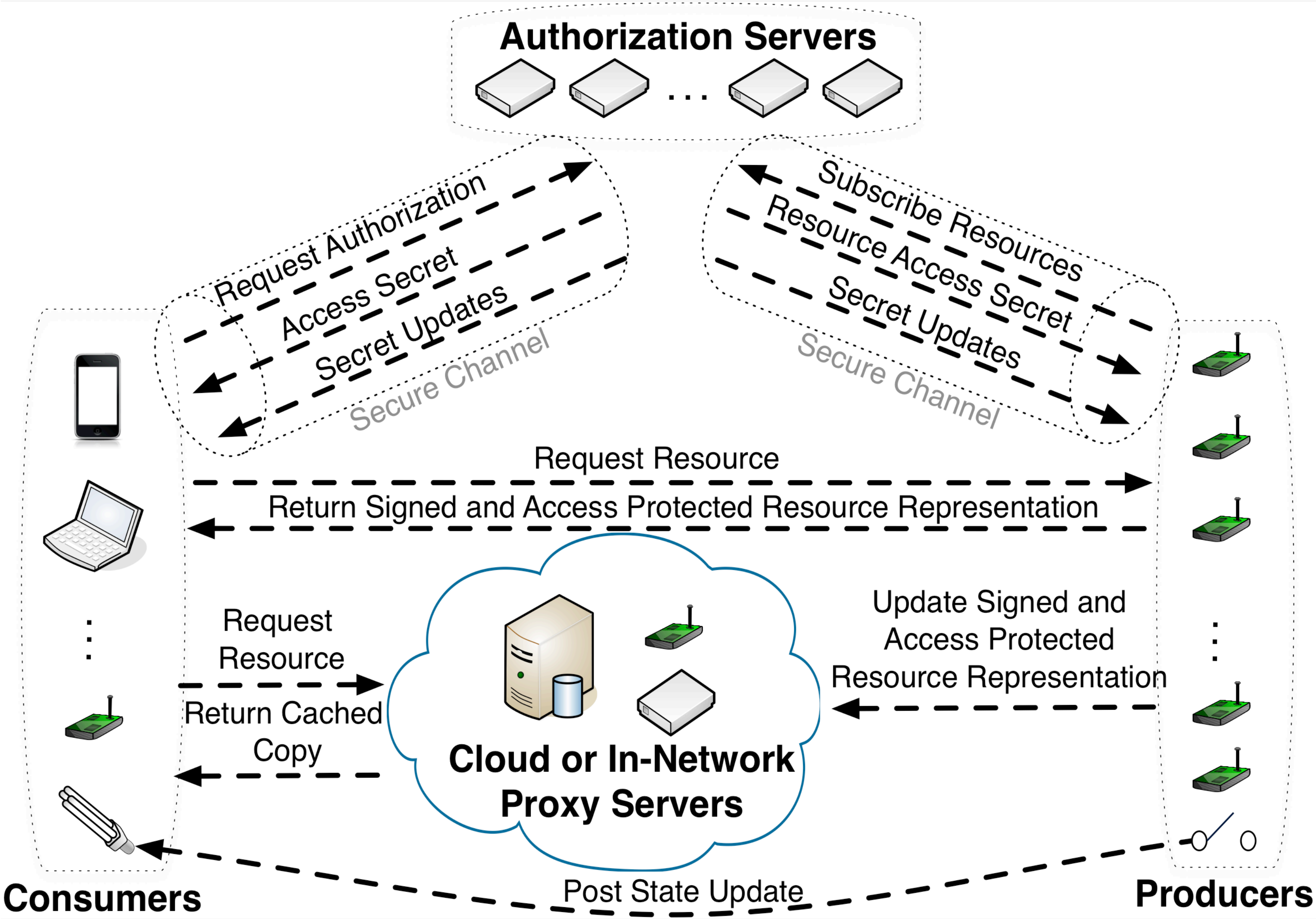
Object Security Architecture for the Internet of Things [1]

- **Idea 2:** Move the burden of security handshake away from sensors
  - Introduce a **semi**-trusted, non-constrained third party that will do the hard work
  - Sensors respond with secured objects (resource representations) regardless of the identity of the client

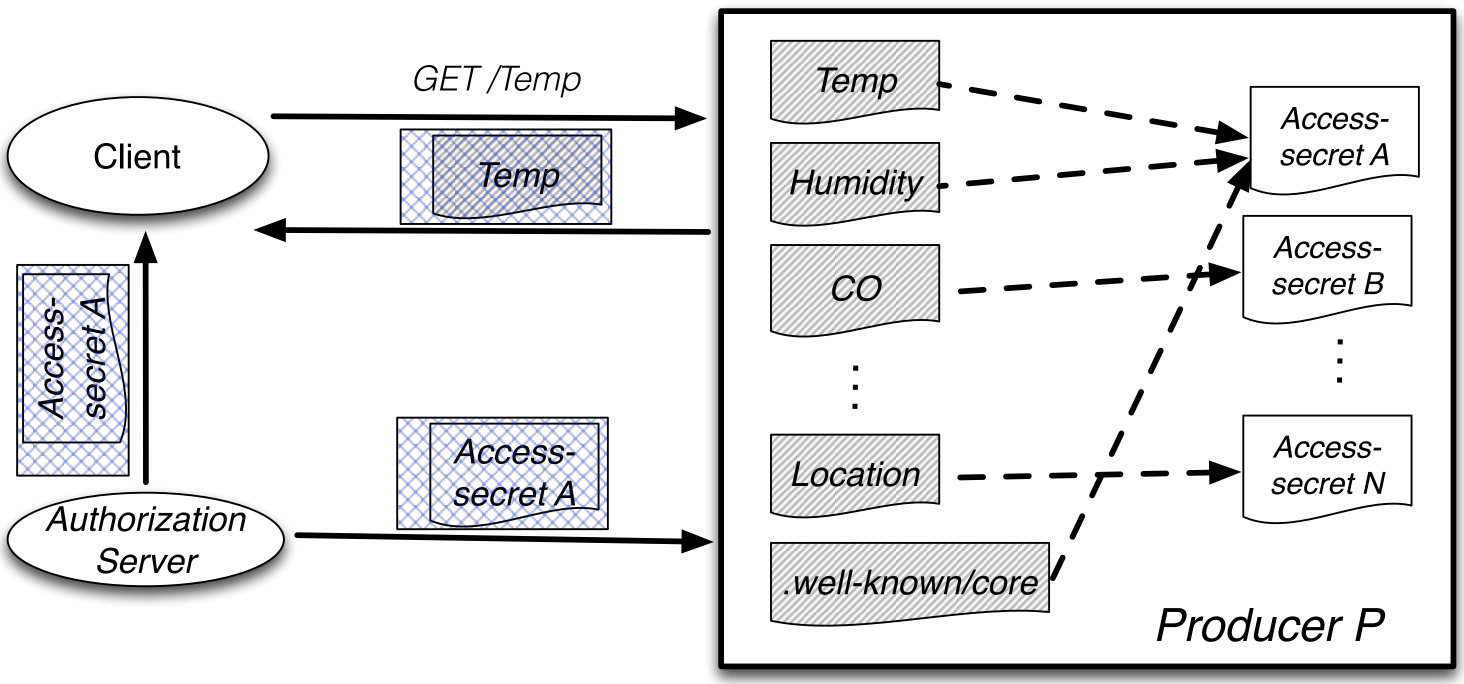
- **Idea 3:** Jointly approach problems of End-to-End security and Authorization
  - Split confidentiality and authenticity trust domains
  - Confidentiality used to provide access-control for group members
  - Authenticity strongly tied to the originator of the information (individual sensor)

[1] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, R. Guizzetti,
OSCAR: Object Security Architecture for the Internet of Things, in: WoWMoM, IEEE, 2014, pp. 1–10.

OSCAR – dive deep (1/2)



OSCAR – dive deep (2/2)



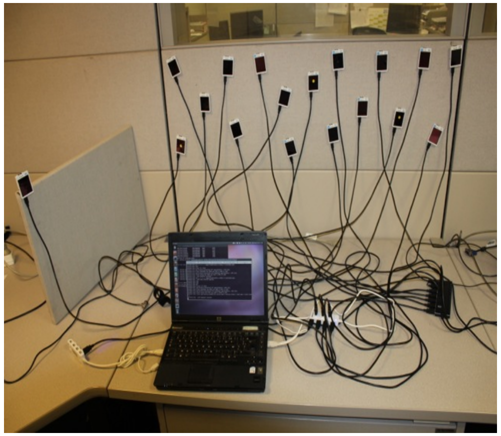
Resource representation pre-signed with P's private key

On-the-fly symmetric encryption with key derived from access-secret

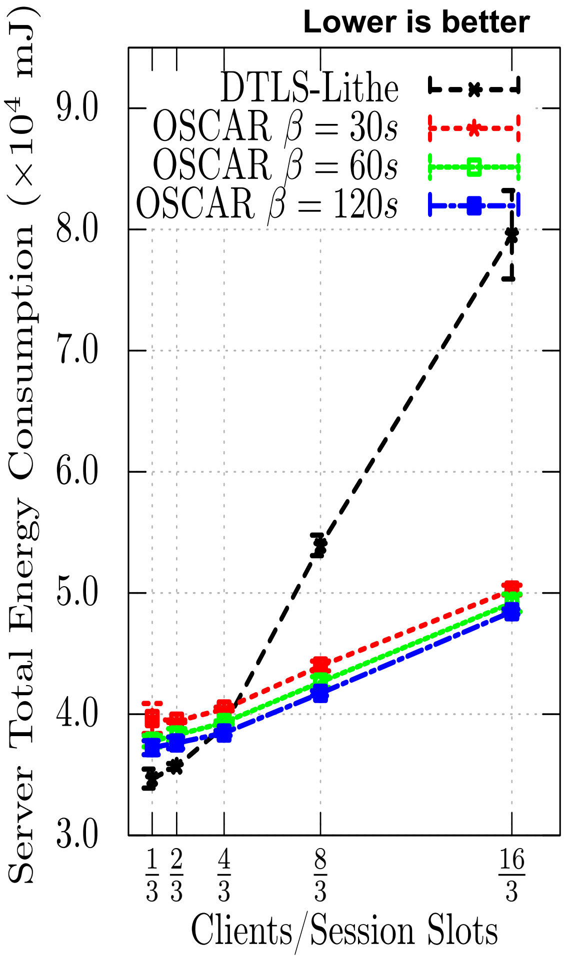
CoAP + OSCAR

- CoAP + OSCAR features:
  - Group communication i.e. multicast support ✓
  - Asynchronous message exchanges ✓
  - Proxy and caching capabilities ✓
  - Low overhead ±
  - Header mapping to HTTP ✓
  - End-to-End Security ✓
  - Authorization and Access Control ✓

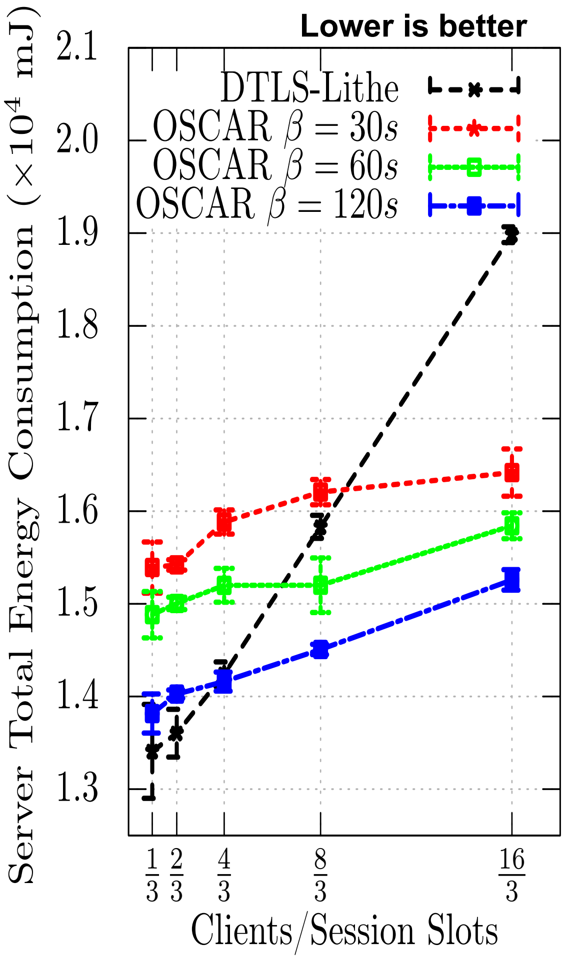
Sensor-side Total Energy Consumption



WiSMote (MSP430)



ST GreenNet (ARM Cortex M3)



OSCAR performs better asa client # >> slot #

GreenNet

Conclusions & Future Work

- E2E security and authorization framework that supports application requirements
- E2E security even in presence of application-level gateways
- Particularly useful for use-cases where high number of clients per sensor is expected
    - Smart city a very good example
- Future extensions
    - Use-cases that require streaming where constant digital signing is unfeasible
    - Key management and authorization policies

life.augmented

L I G

Hvala!*

Questions?

*Thanks!