Implementing End-to-End Security in Internet of Things

Vishwas Lakkundi

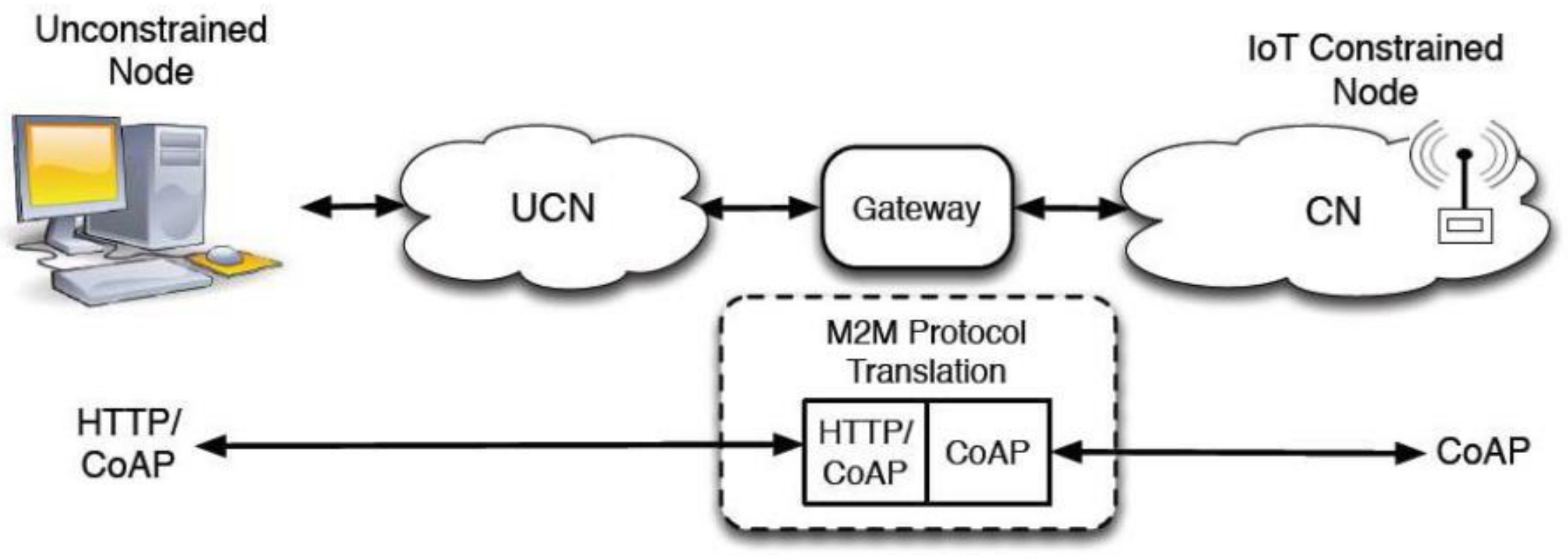
Altiux Innovations Private Limited

Bengaluru, INDIA

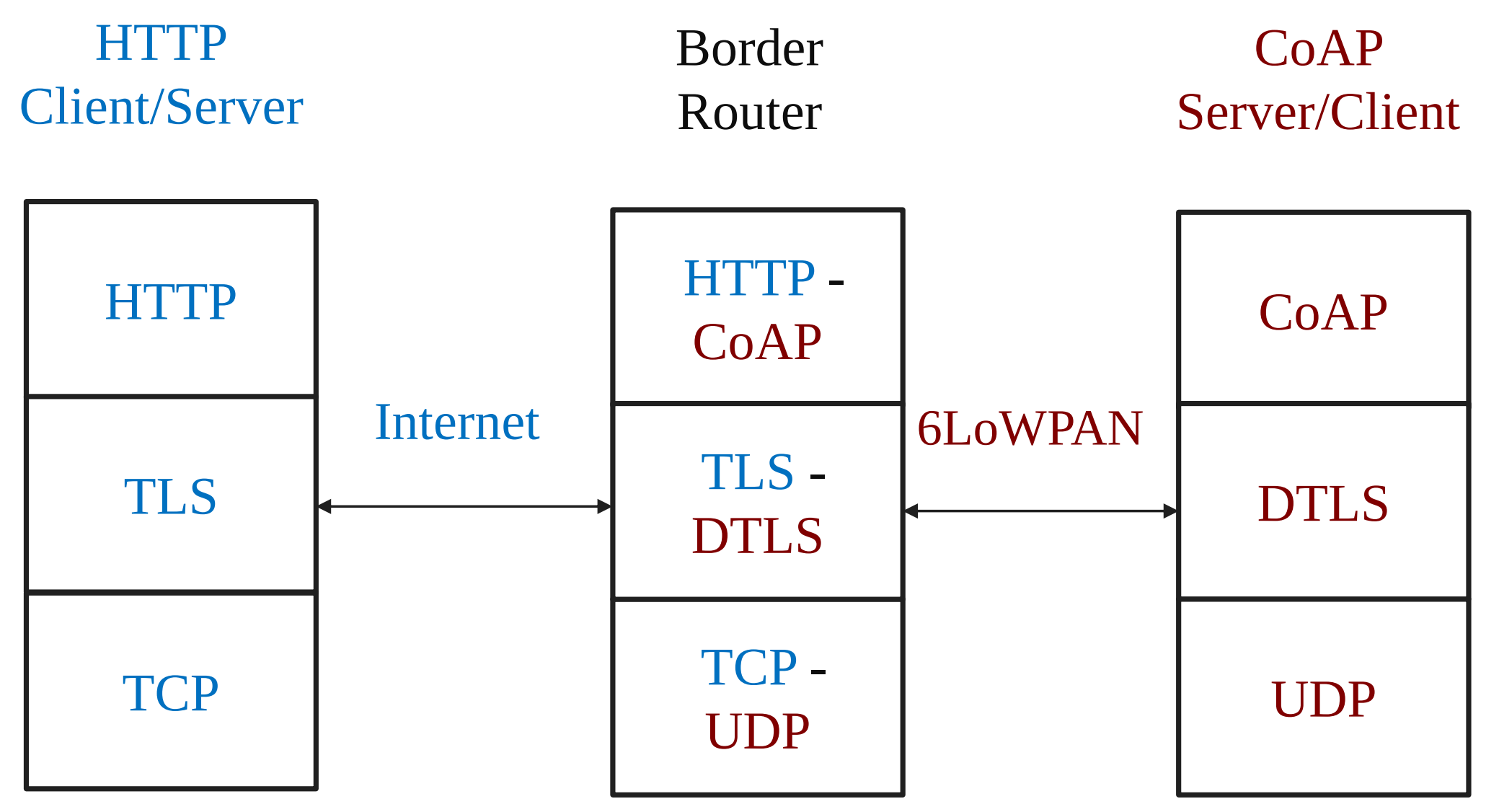
1. Abstract

Security is fast emerging as a key area of focus in the Internet of Things. Lightweight implementations of the required security features are necessary considering the resource constrained nature of the underlying nodes and networks. At the same time, it is essential that such implementations are robust, reliable and efficient. Security can be provided at different layers of the underlying protocol stack. This poster addresses these requirements by providing a end-to-end security framework for implementing a lightweight version of the DTLS protocol in the CoAP-based Internet of Things. In addition, this lightweight security approach is illustrated with a real-world application scenario and its performance analysis. It also provides an overview of the ongoing standardization activities in the IoT security domain.

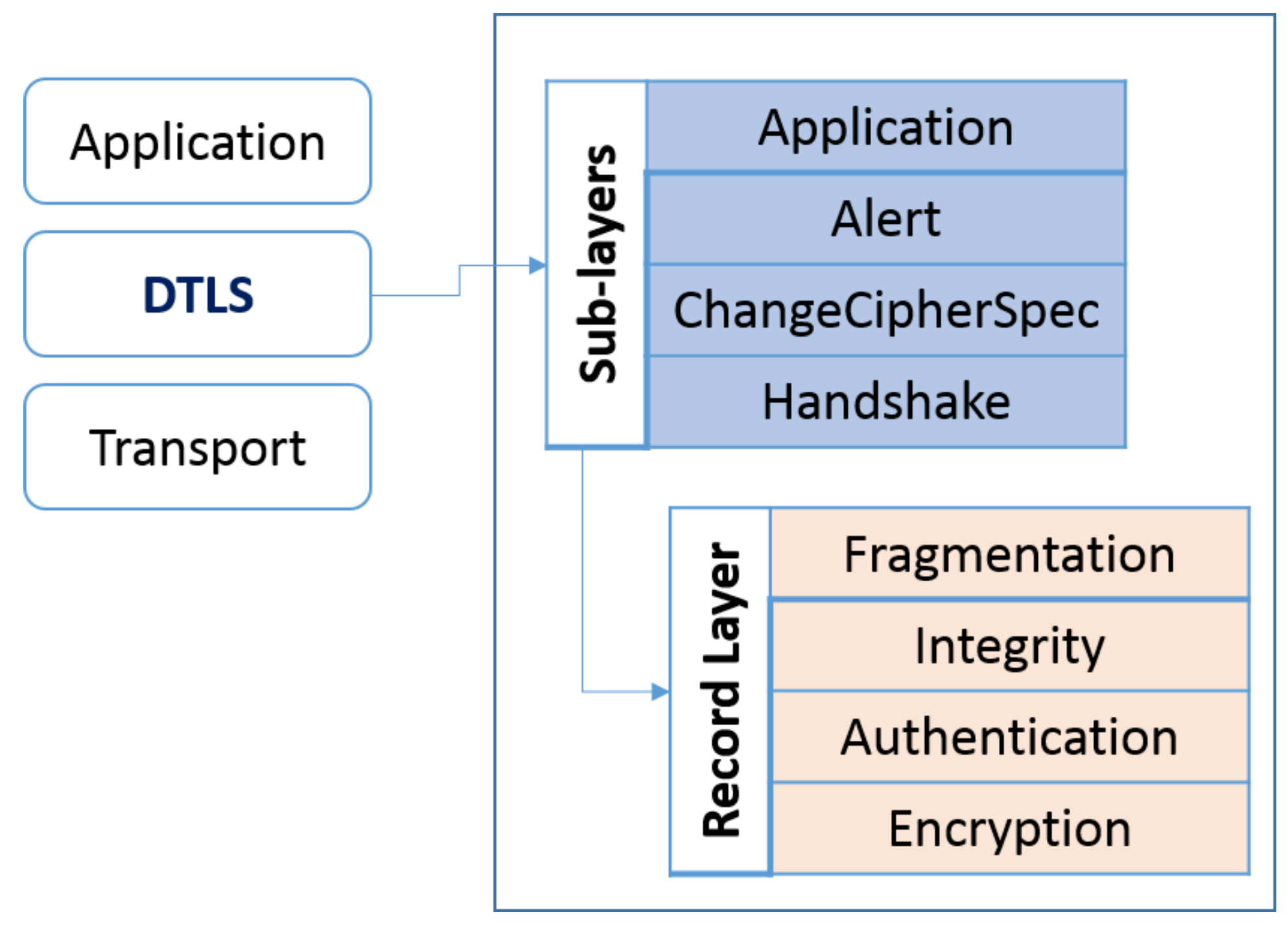
4. Security in IoT - Protocols



IoT Communication Scenario

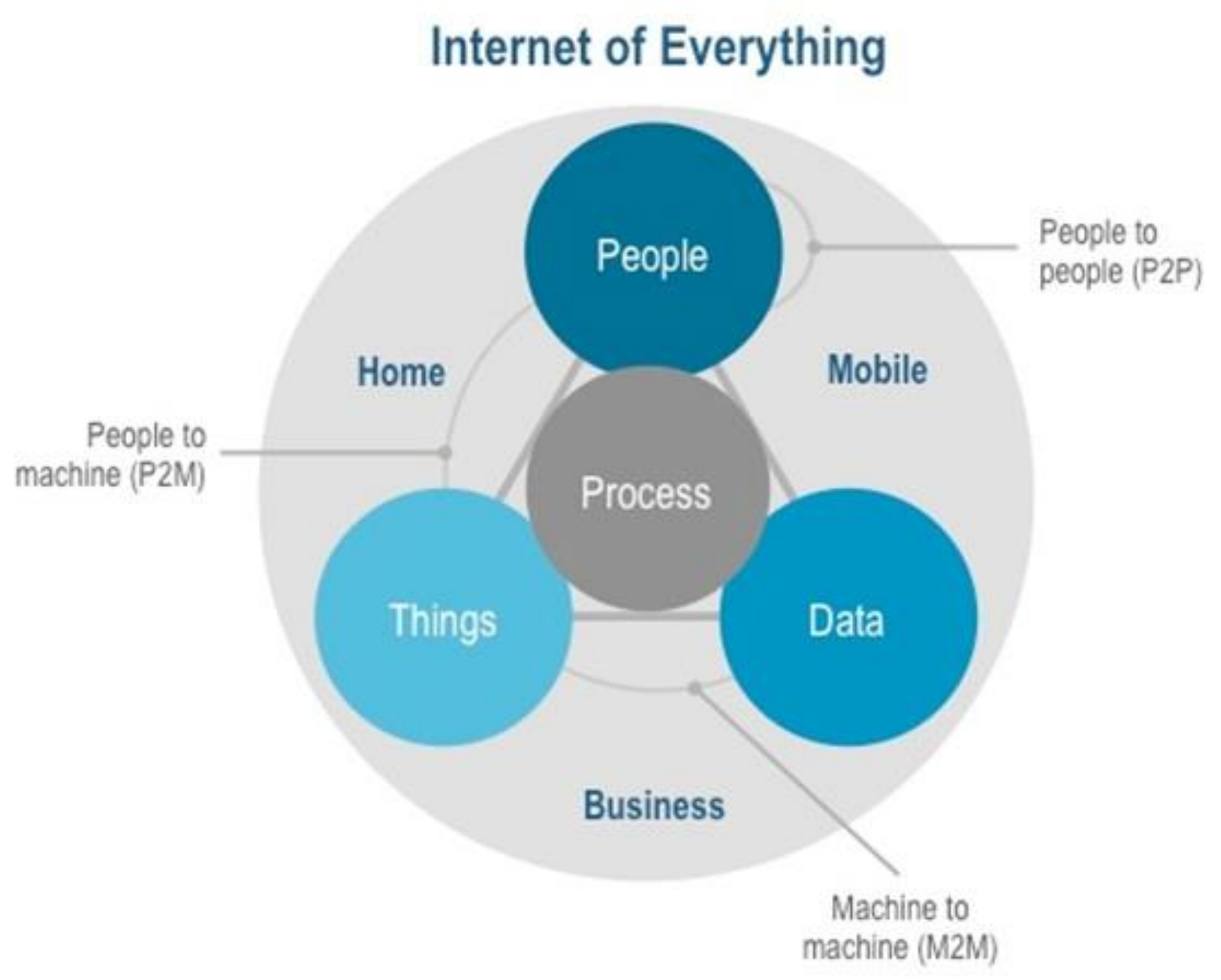


End-to-End Security: Protocol Architecture



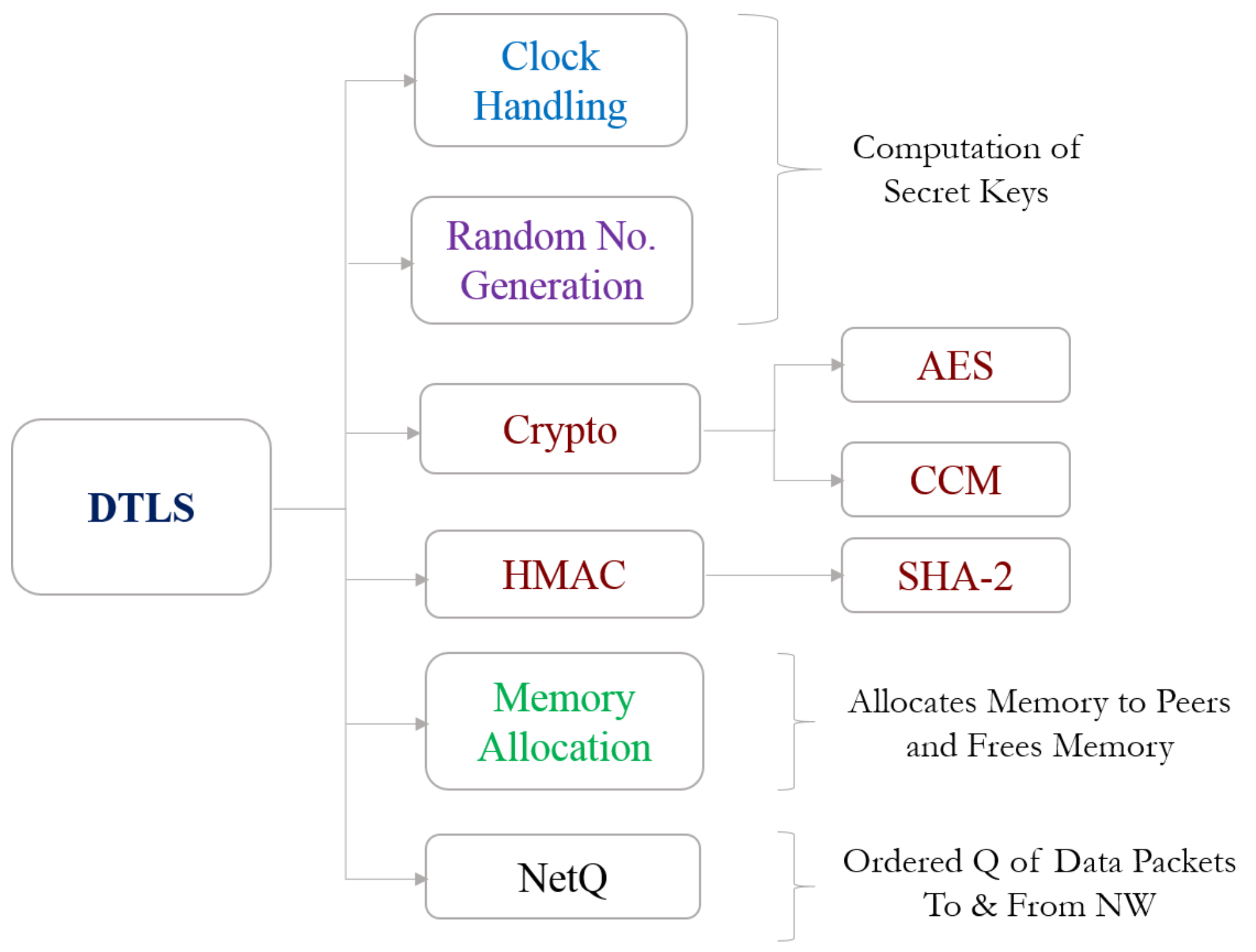
Datagram Transport Layer Security: Overview

2. Internet of Things

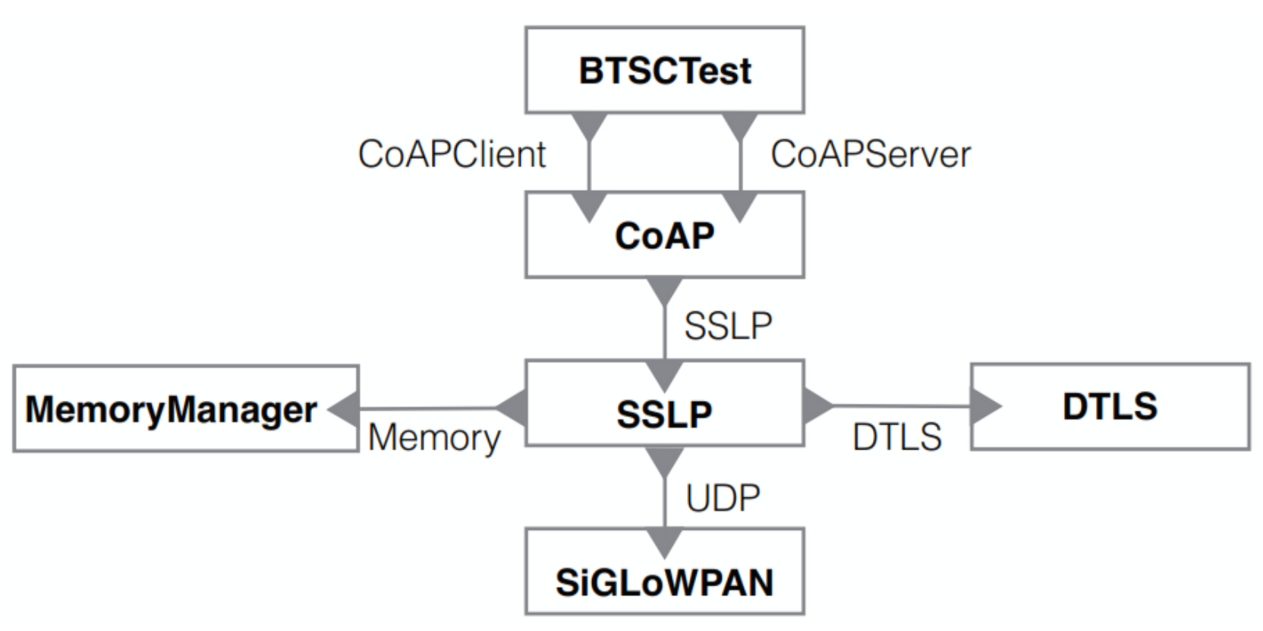


5. Lightweight DTLS

- Supports pre-shared key (PSK) based security
- Supports advanced encryption standard (AES)
- Supports HMAC-SHA2 base hashing algorithm
- IETF Class-1 compliant (~100 KB ROM, ~10 KB RAM)

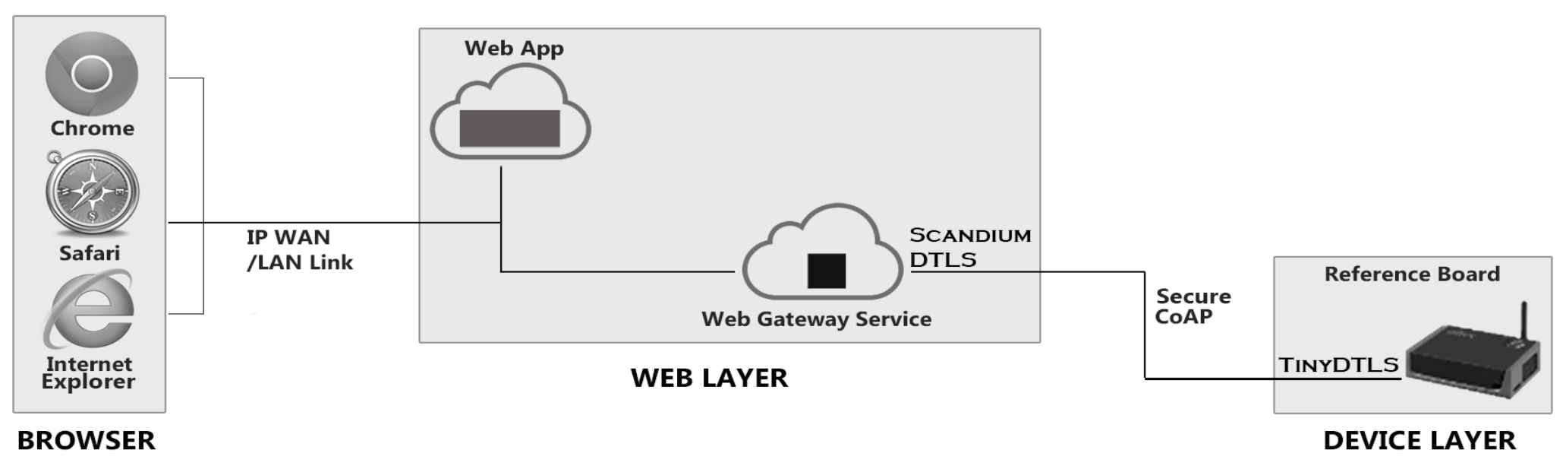

DTLS
Clock Handling
Random No. Generation
Computation of Secret Keys
Crypto
AES
CCM
HMAC
SHA-2
Memory Allocation
Allocates Memory to Peers and Frees Memory
NetQ
Ordered Q of Data Packets To & From NW

DTLS Implementation – Protocol Library



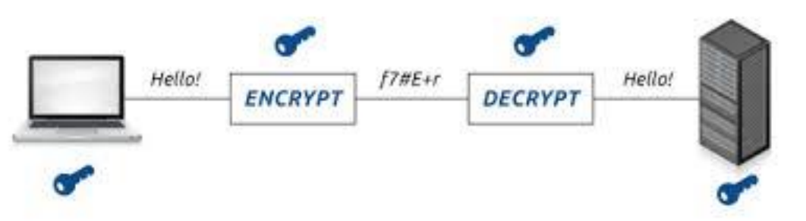
Security Framework and Interfaces

7. Application Scenario



3. Security in IoT

Data Encryption



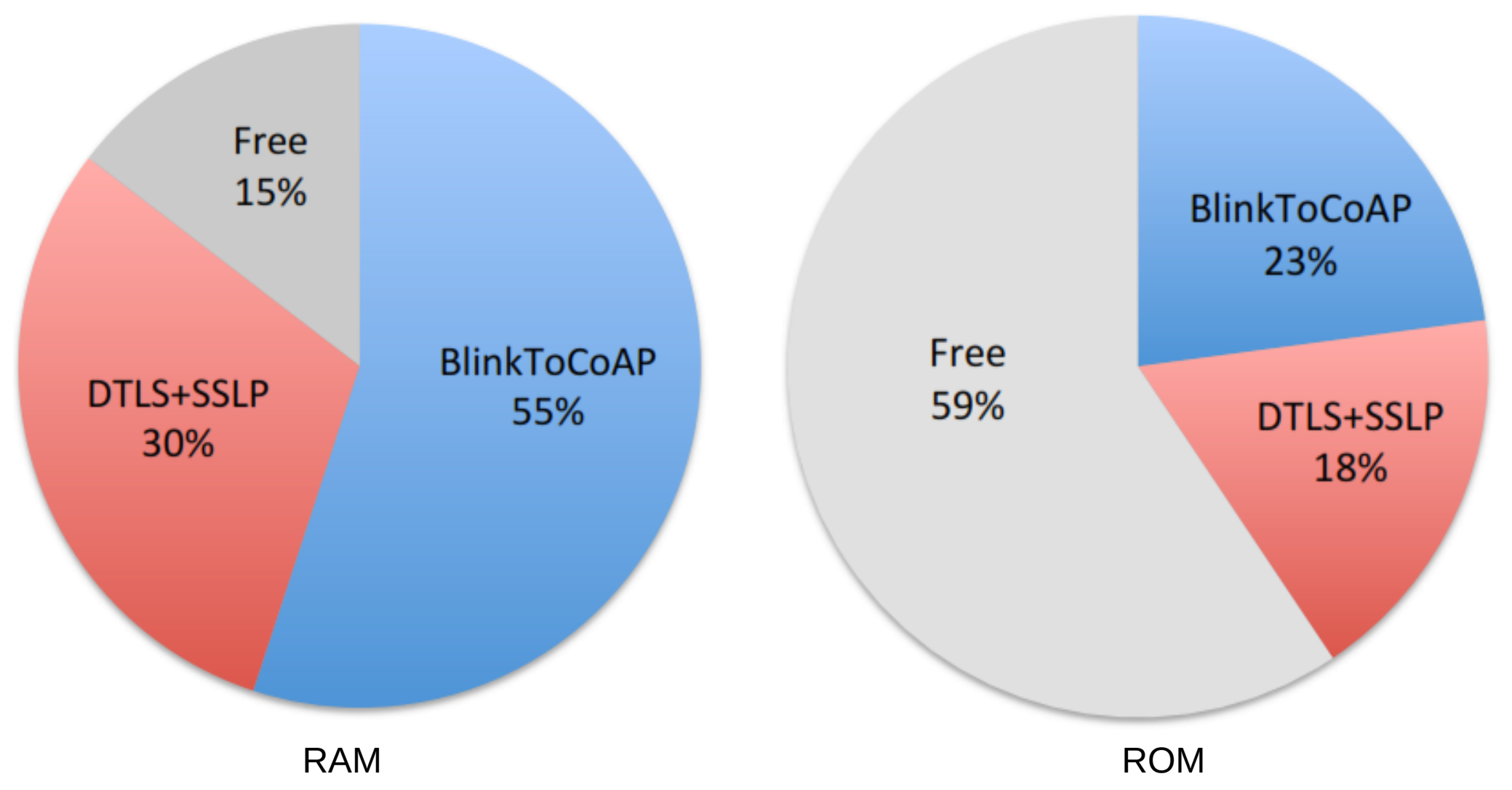
Source Authentication

Message Integrity

IoT Devices:
- Pervasive in Nature
- Huge Amount of Data
- Resource Constrained
  - Available Memory
  - Computational Capability
  - Power Management

Security Techniques:
- Lightweight Crypto Primitives
- Effective Key-Management

6. Performance Analysis

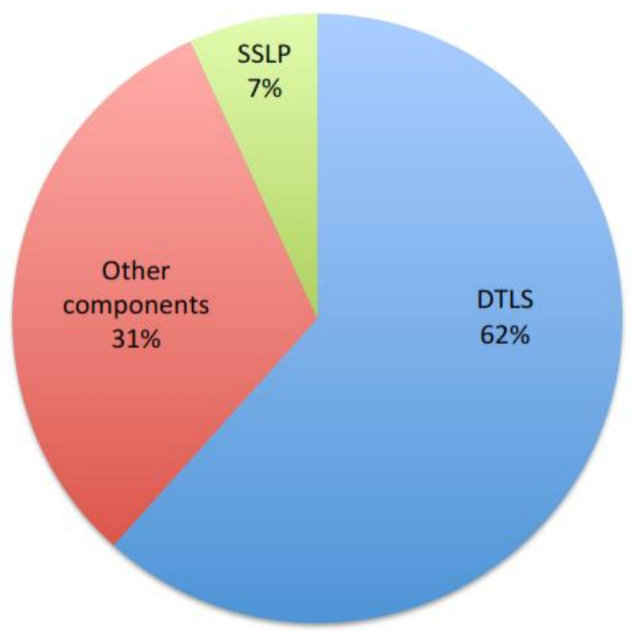


Memory Footprint

	Frame [bytes]	UDP payload [bytes]
Unsecured Request	30	13
Unsecured Response	24	7
Secured Request	59	42
Secured Response	53	36

Packet Overhead

- CoAP overhead: 17 bytes per frame
- DTLS overhead: **29** bytes extra



Energy Consumption

8. Standardization Activities

- DICE: **D**TLS **I**n **C**onstrained **E**nvironments
  - Currently being standardized by **IETF**
  - Propose a **minimal DTLS profile** for use in IoT scenarios
  - Enables DTLS record layer for secure **multicast** transmissions

  Investigates **practical issues** around DTLS **handshake**
- DICE does NOT intend to modify DTLS **state machine**
- Out of scope: **key management** and **multicast sessions**

- ACE: Authentication and Authorization for Constrained Environments
  - Currently being standardized by **IETF**
  - Identifies authentication and authorization mechanisms suitable for resource access in constrained environments
  - Produces use cases and requirements

References

- *BlinkToSCoAP: An End-to-End Security Framework for the Internet of Things*, IEEE COMSNETS 2015.
- *Lightweight DTLS Implementation in CoAP-based Internet of Things*, ADCOM 2014.

Marie Curie Alumni Association – Annual General Assembly, 6-7 February 2015 – Porto, Portugal