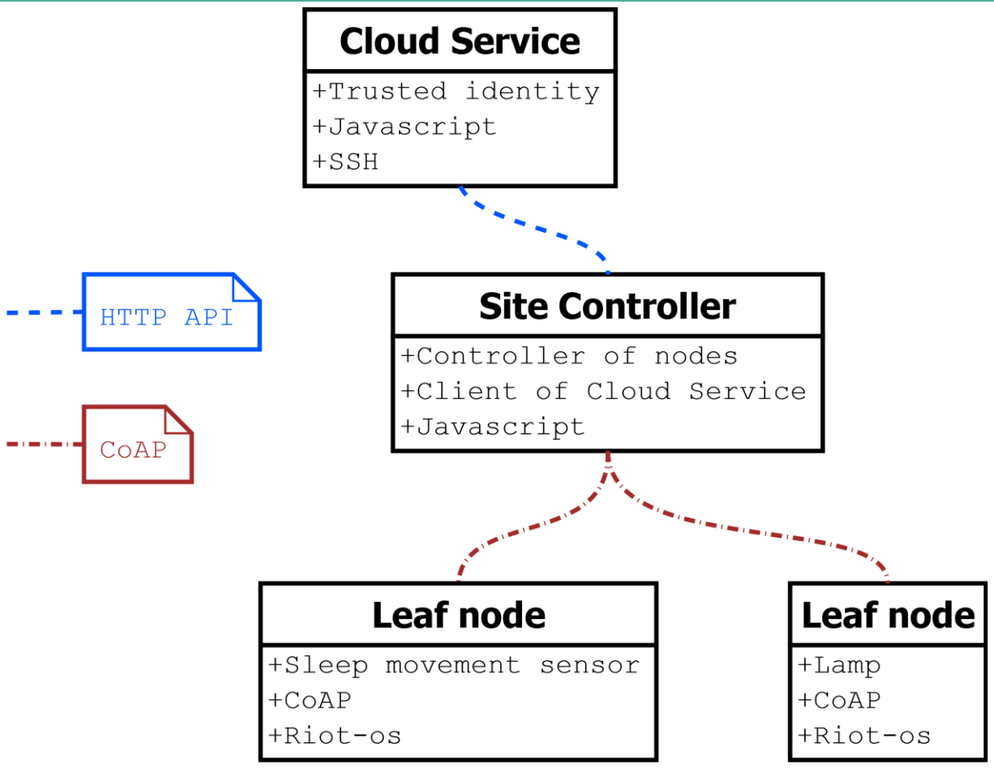
Masterproef industriële ingenieurswetenschappen

Public-key cryptography with mutual authentication for IoT platform

Jori Winderickx

Academiejaar: 2014-2015

Introduction



How to implement the IoT platform of ELL-i with IP-enabled security?

Platform:
- Cloud Service
- Leaf node
- Site Controller

Objectives:
- Interoperable
- Lightweight
- Open source
- Trust

Methods

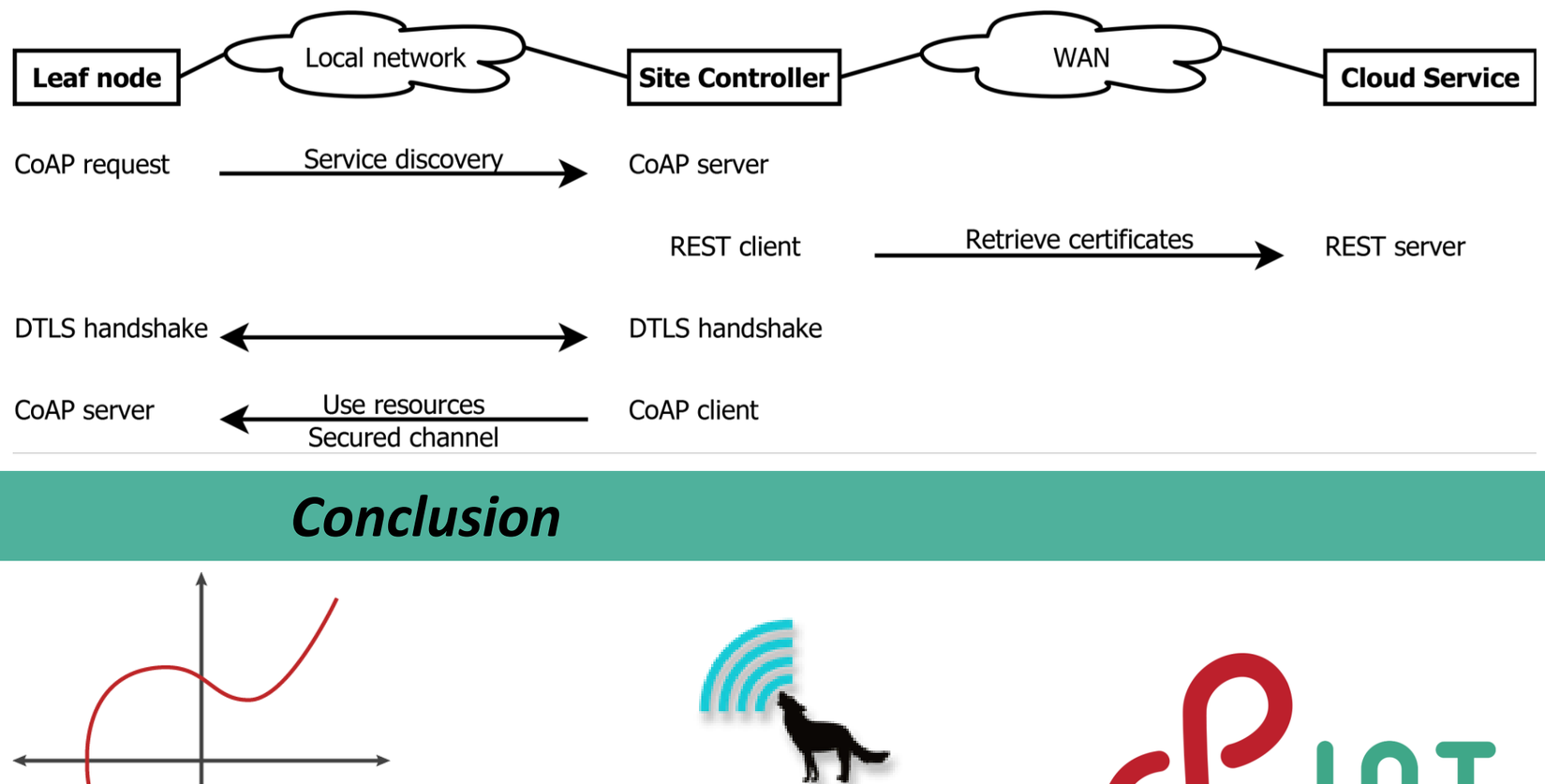
Interoperable:
- Standards

Trust:
- Mutual authentication

Lightweight:
- Public-key algorithm
- Authentication process
- Libraries
- Traffic encryption algorithm
- Key-establishment algorithm

Results

- **DTLS**
- **X.509 certificate**
- **ECDSA_ECDH_AES_CCM_8**
- **DTLS interface for JavaScript**
- **WolfSSL**



Conclusion

- **Automatic integration**
- **Mutual authentication**
- **Interoperable**
- **Secure connection**
- **Open source**

Promotoren / Copromotoren: Teemu Hakala
Prof. dr. Nele Mentens