6th International
LED professional Symposium +Expo
Sept 20-22, 2016 | Bregenz

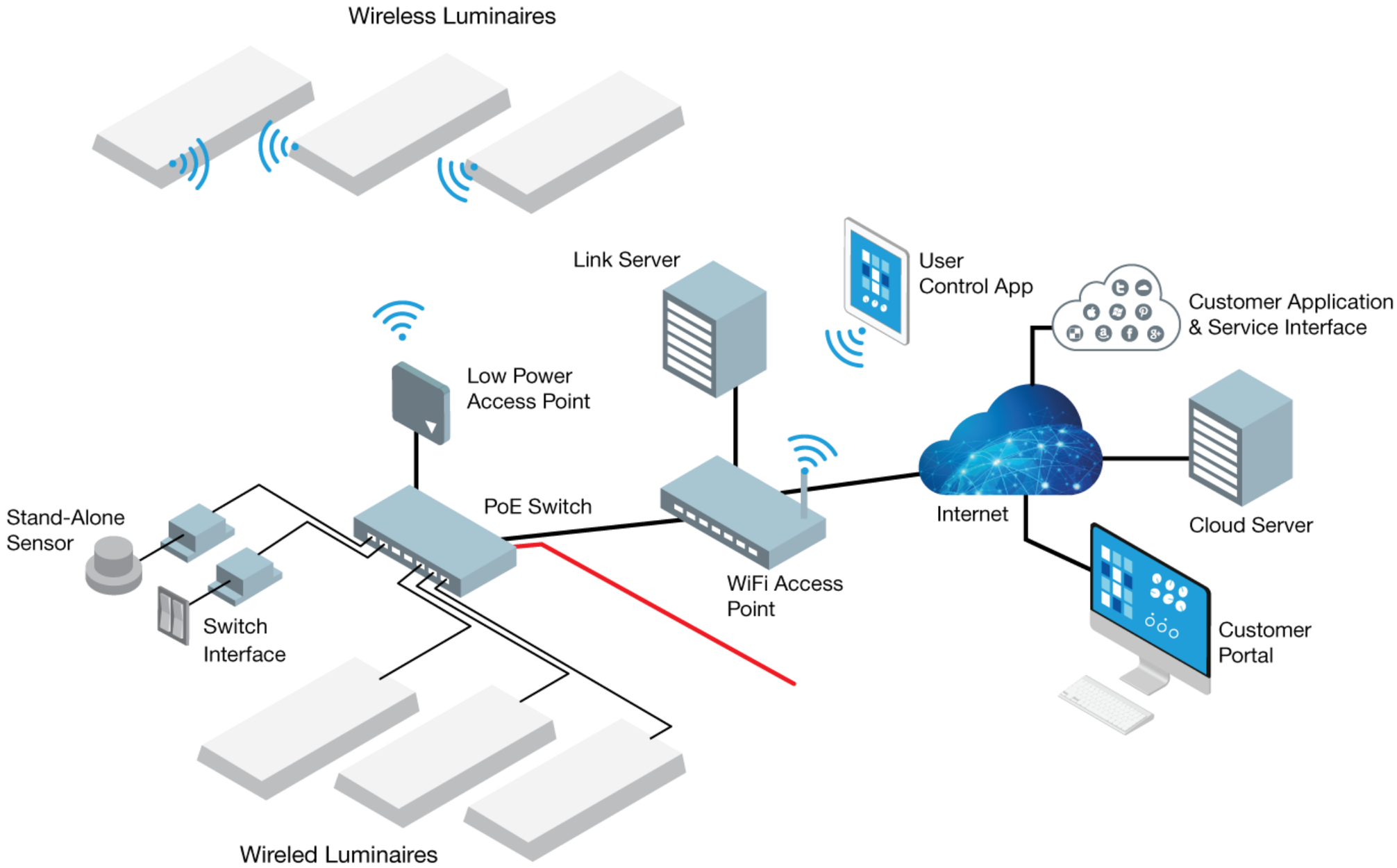
Security for lighting in IoT – group communication

Abhinav Somaraju
Tridonic

Table of Contents

- ❑ The big picture
- ❑ Security in IoT and lighting
- ❑ Group communication security

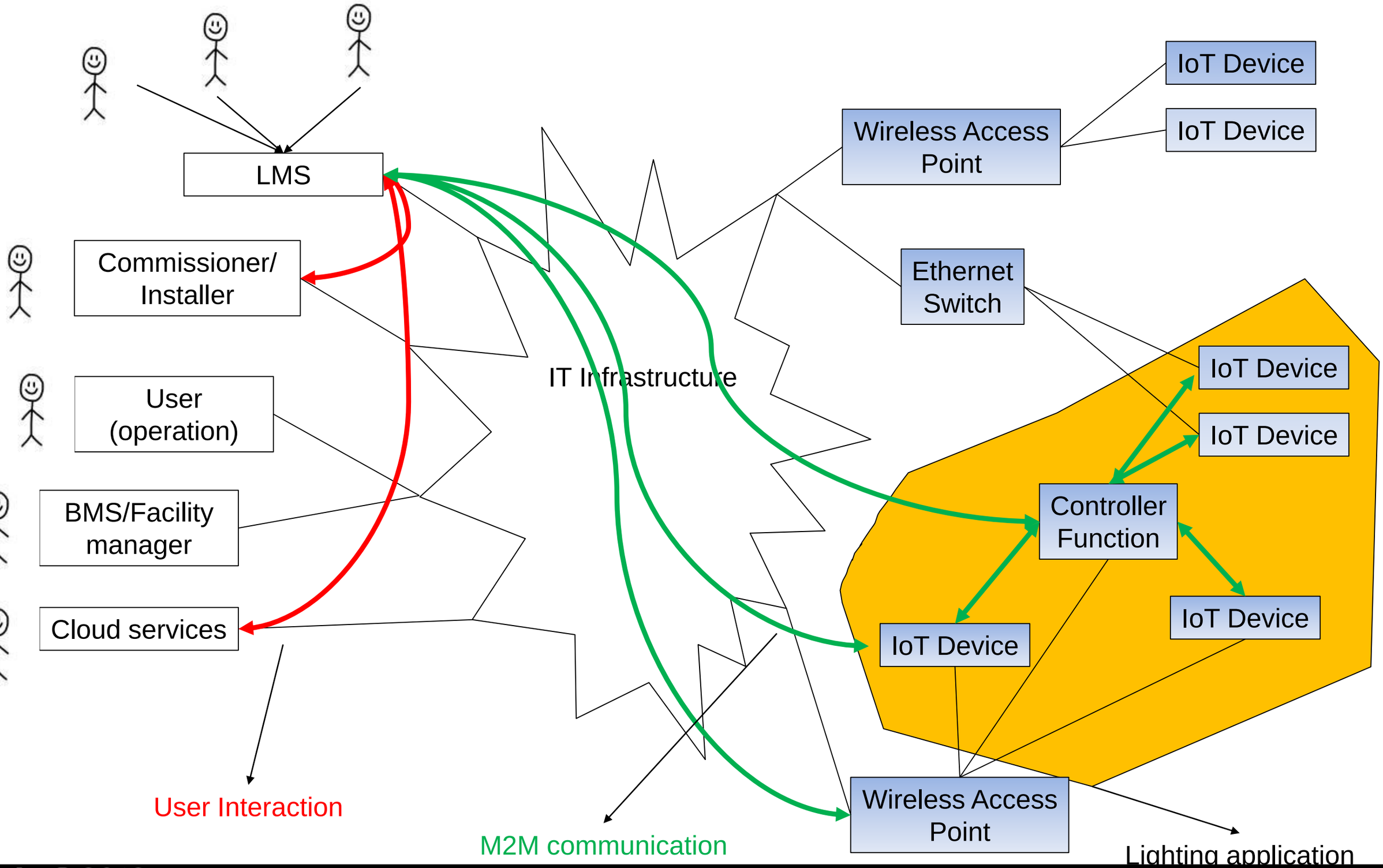
The big picture



Security in IoT – organizational

- Data privacy
- Regulation/compliance
- Incident management
- Human resouces

System Overview

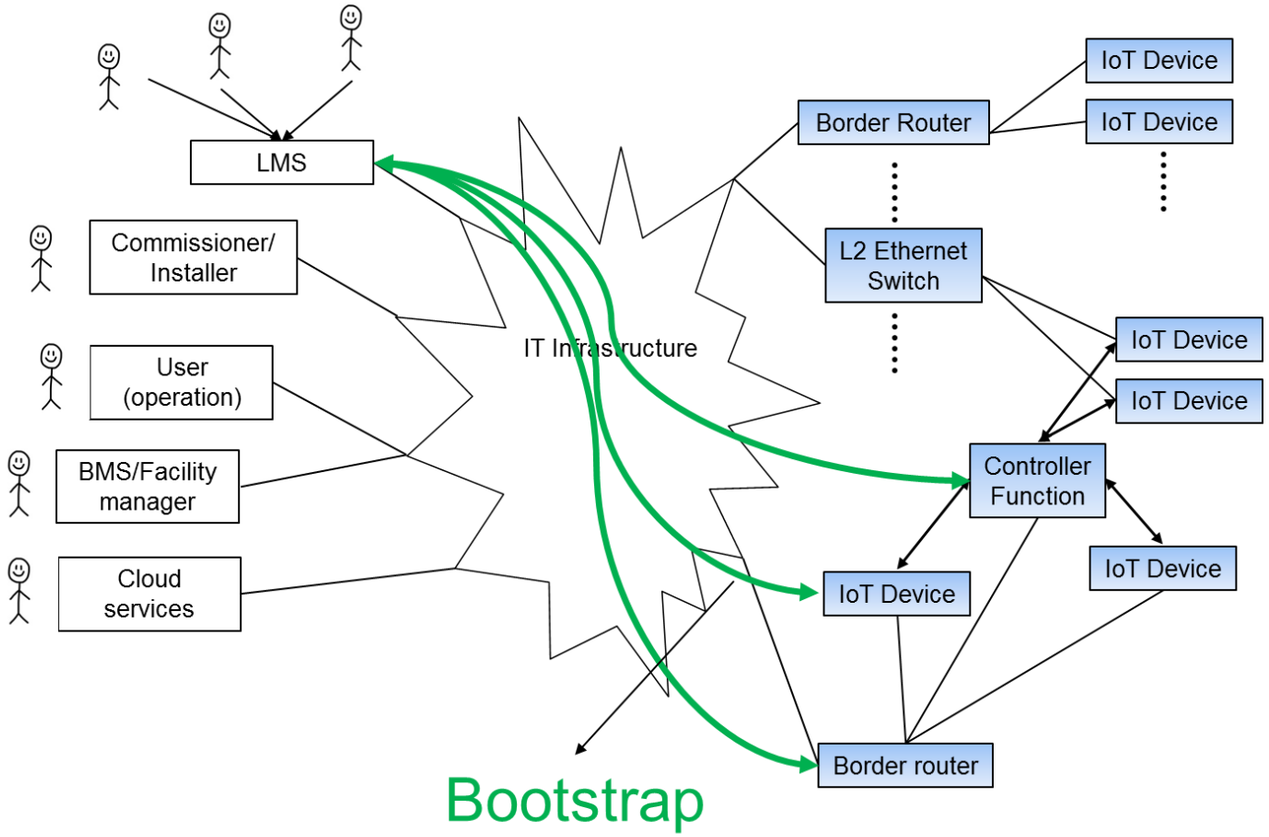


Some security issues – technical

- Initial trust – bootstrap
- Data to cloud
- Peer-to-peer
- Group communication

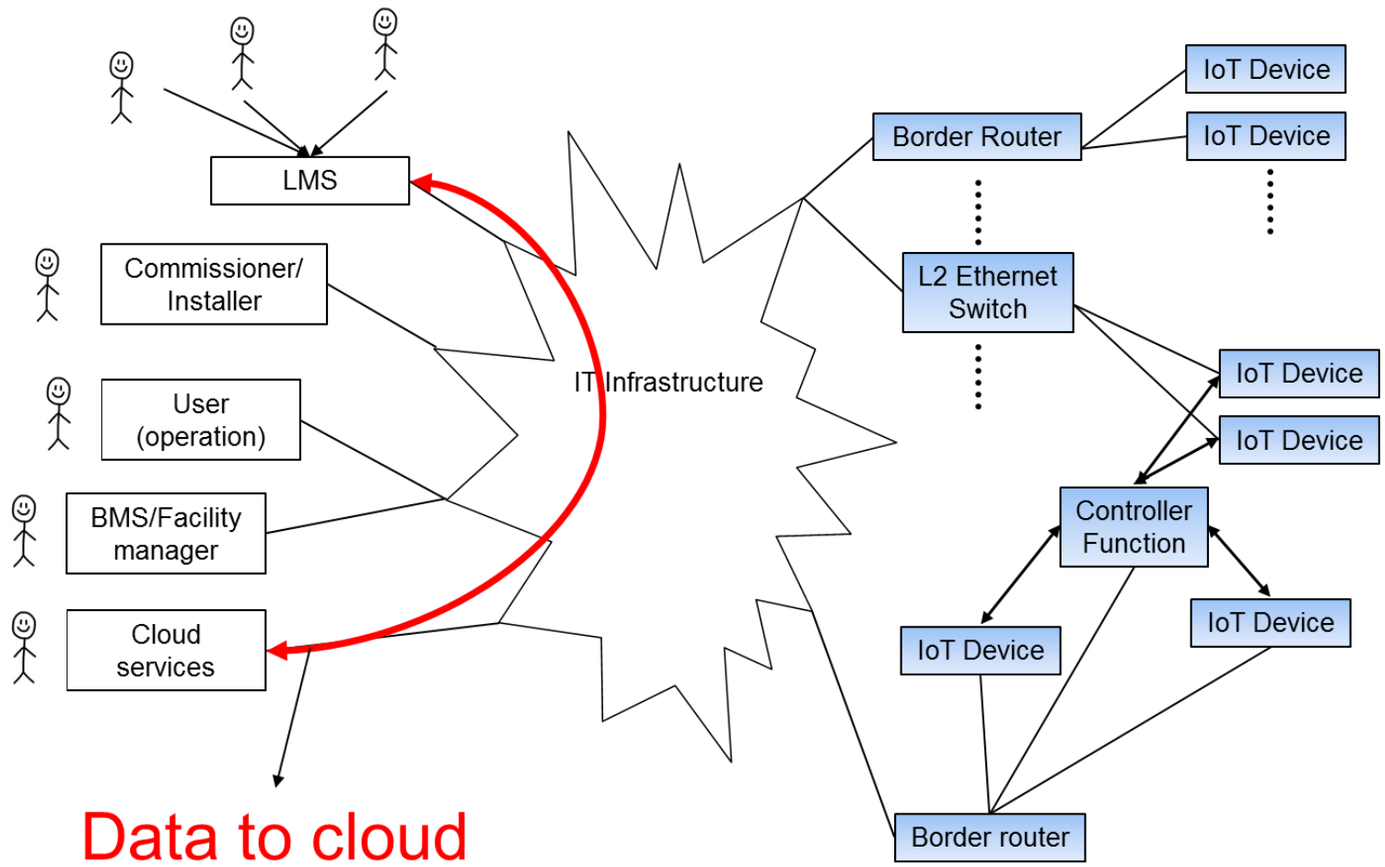
Some security issues – technical

- Initial trust – bootstrap
- Data to cloud
- Peer-to-peer
- Group communication



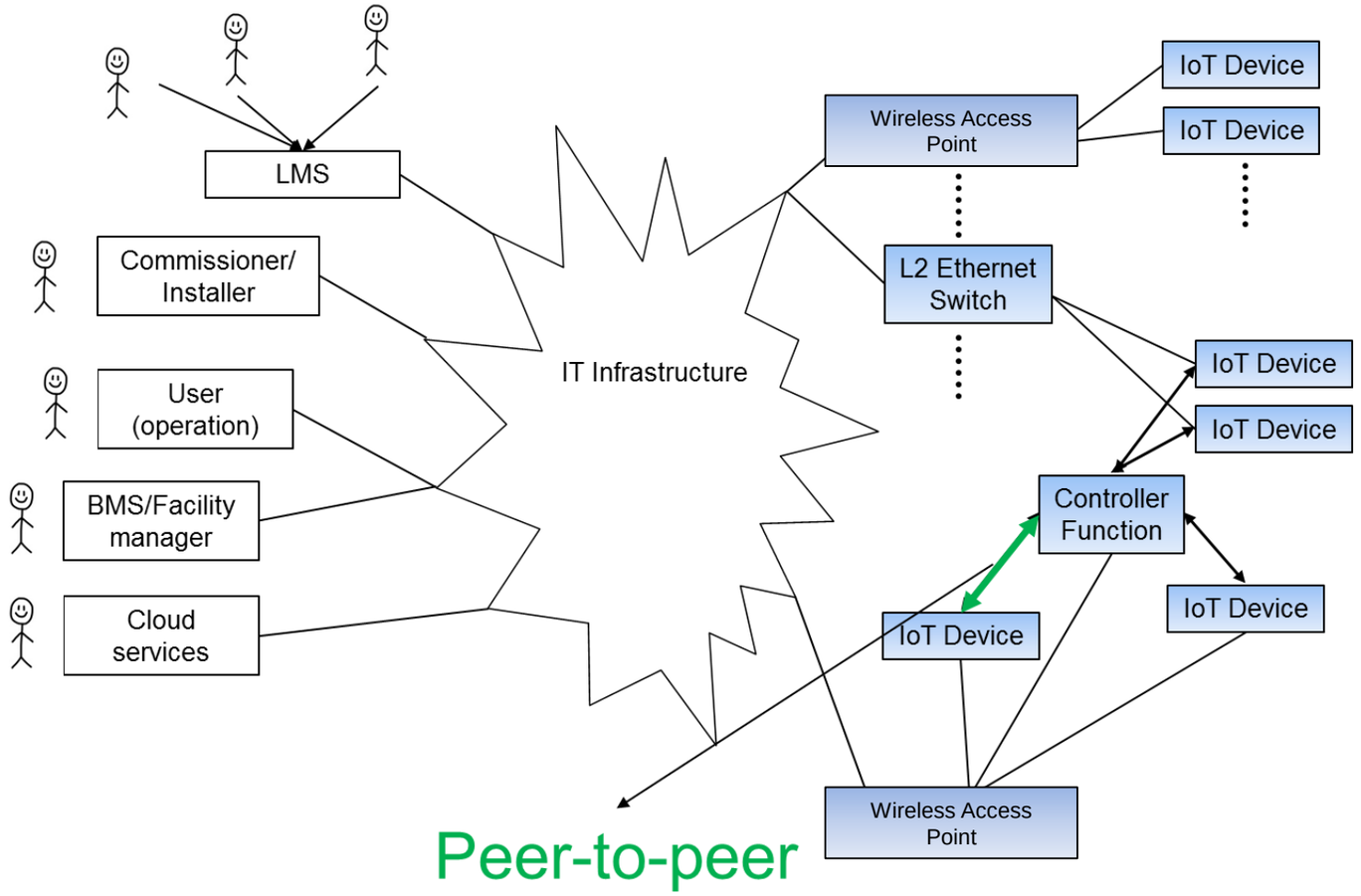
Some security issues – technical

- Initial trust – bootstrap
- **Data to cloud**
- Peer-to-peer
- Group communication



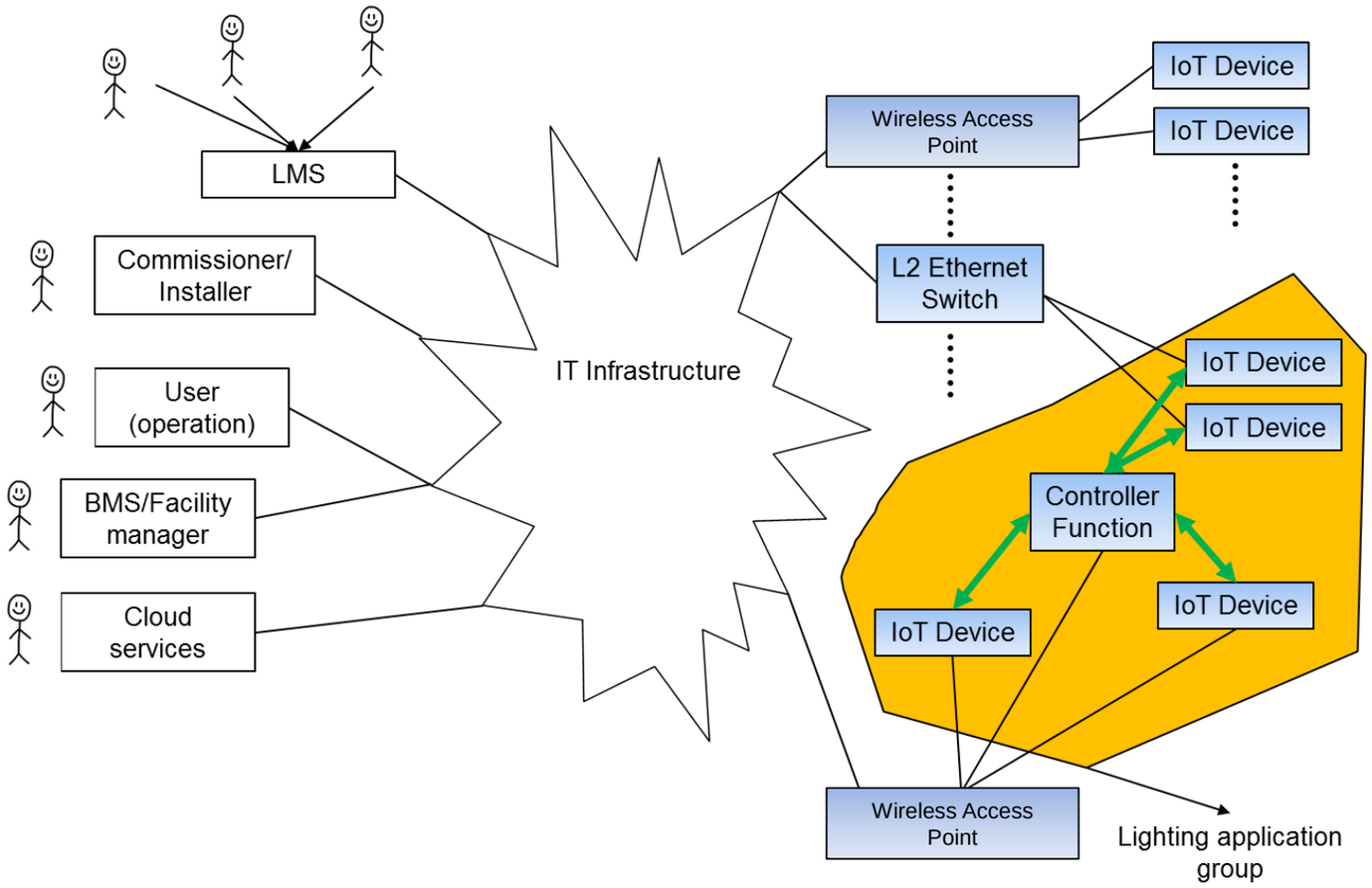
Some security issues – technical

- Initial trust – bootstrap
- Data to cloud
- Peer-to-peer
- Group communication

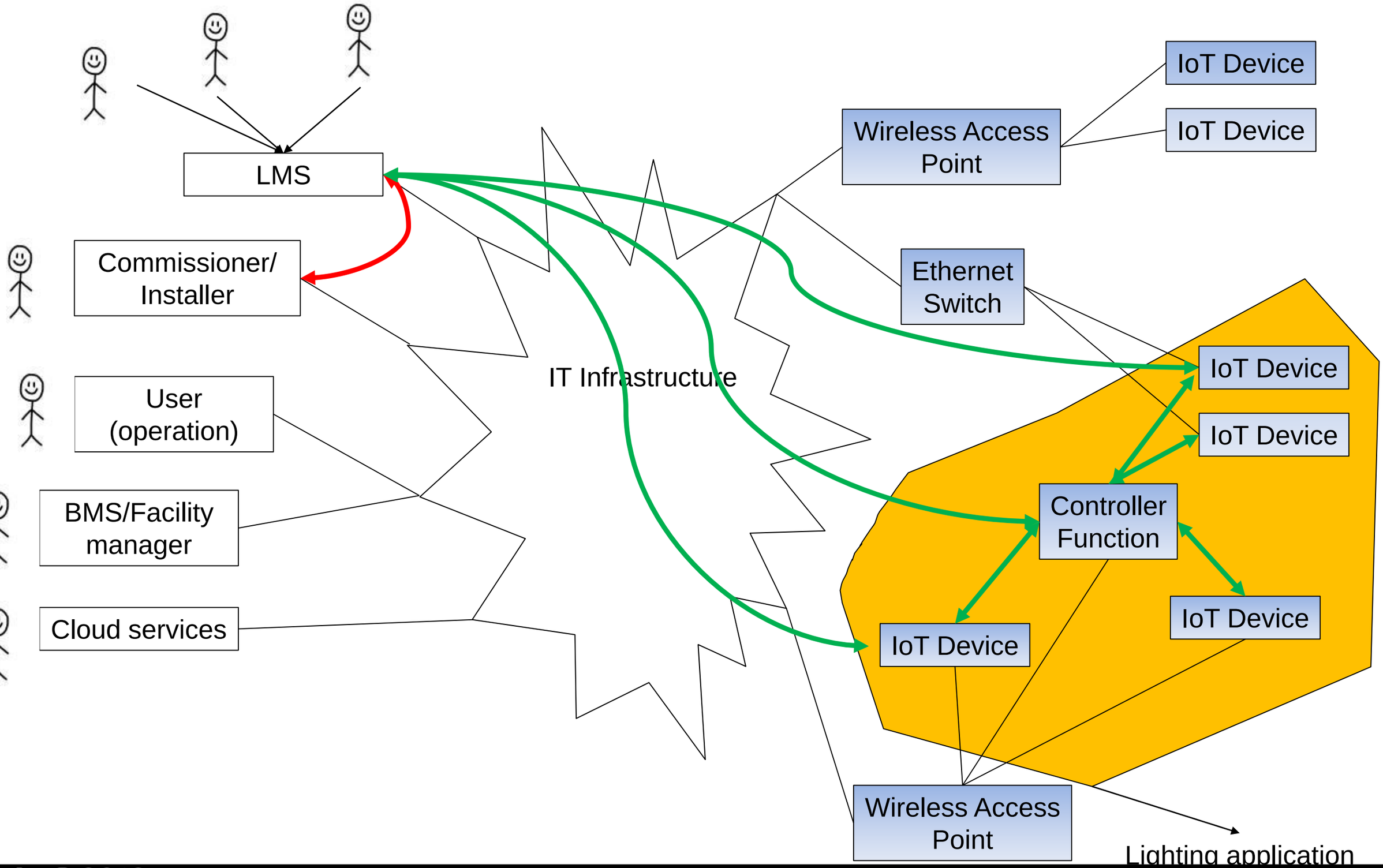


Some security issues – technical

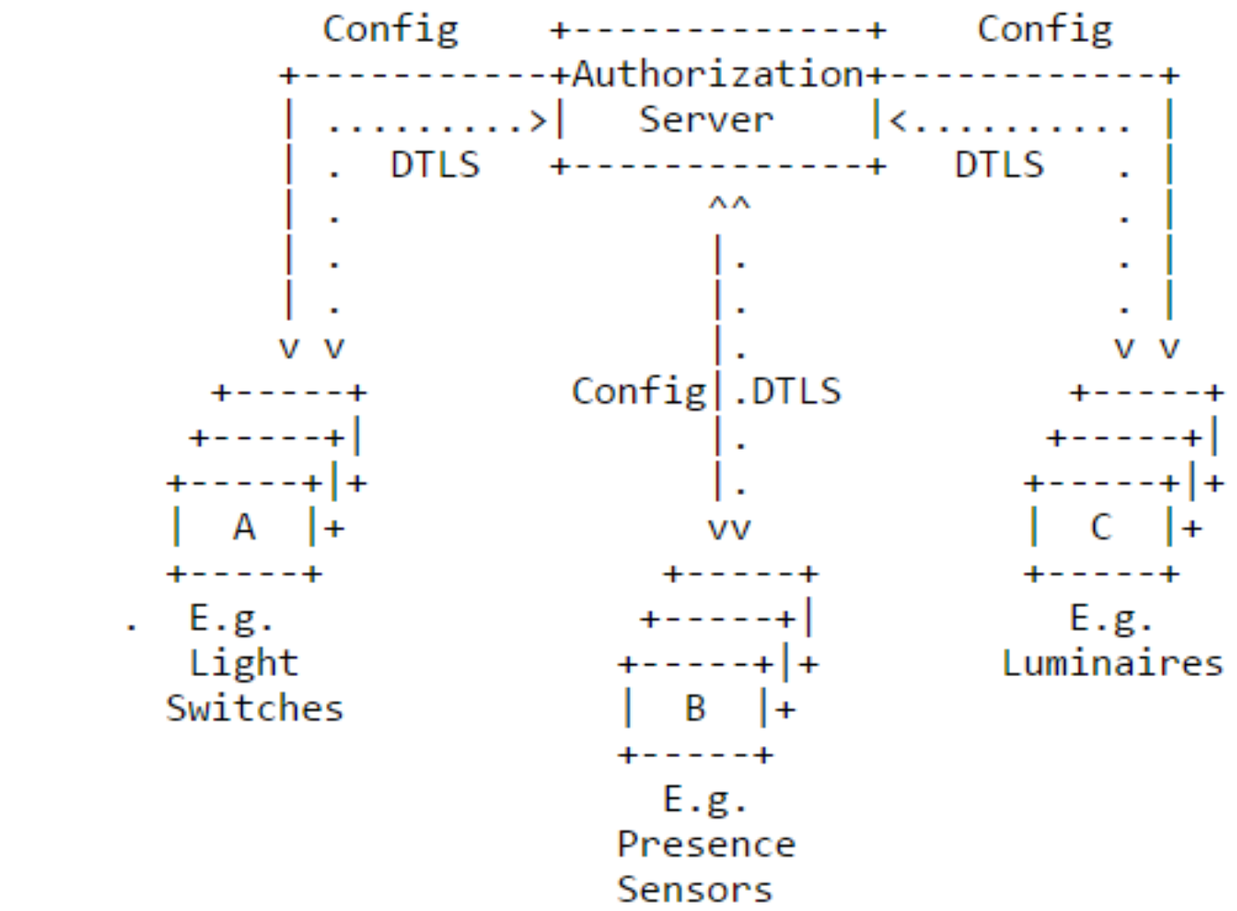
- Initial trust – bootstrap
- Data to cloud
- Peer-to-peer
- Group communication



Commissioner: Authorization



Commissioner: Authorization



Legend:

Config (Configuration Data): Includes configuration parameters, authorization information encapsulated inside the access token (AT-KDC) and other meta-data.

Figure 1: Architecture: Commissioning Phase.

Commissioner: Authorization

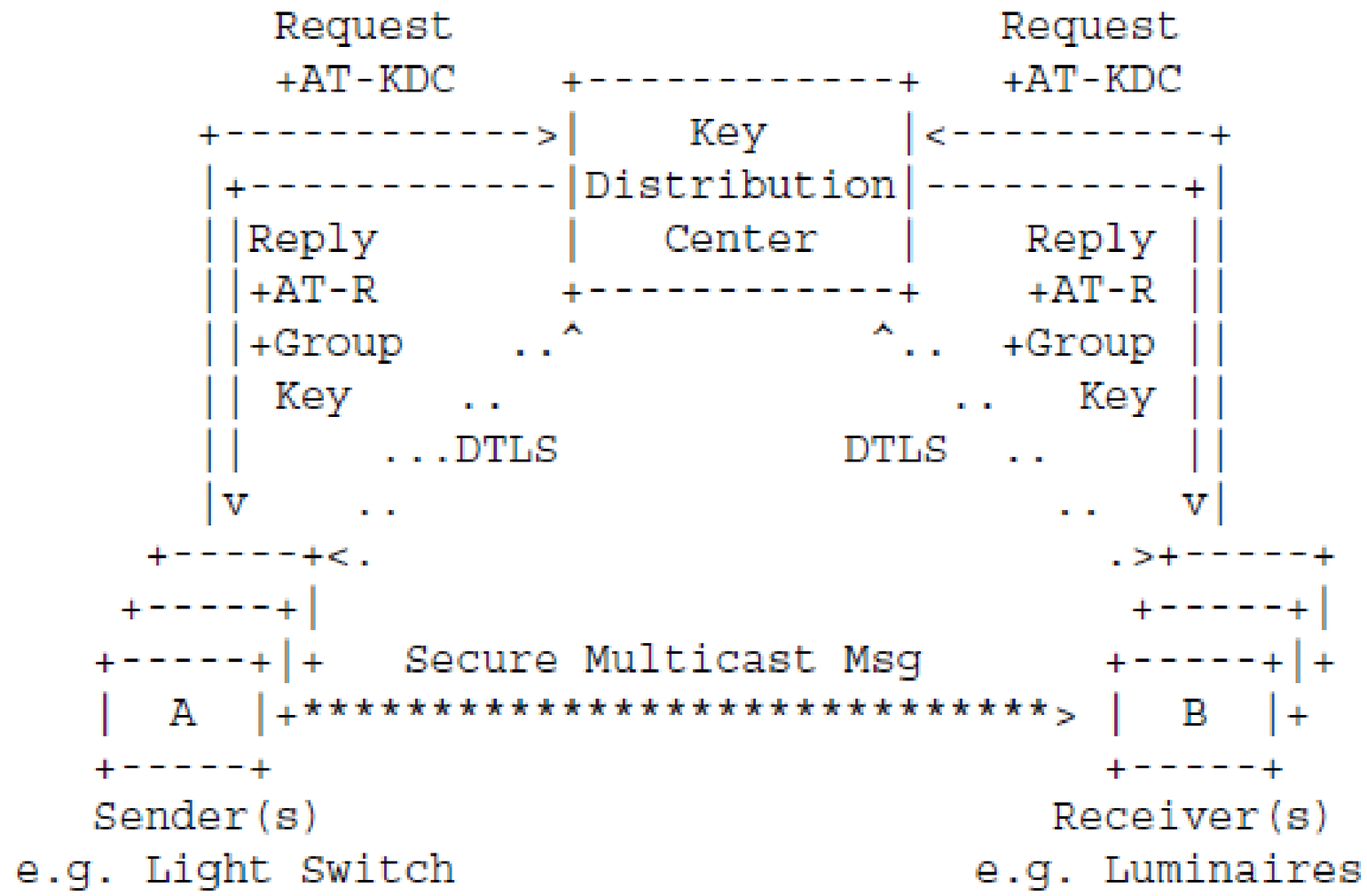


Figure 2: Architecture: Group Key Distribution Phase.

Conclusion

- Organizational vs technical issues
- Several aspects to consider: bootstrap, peer-to-peer, privacy etc.
- Focused on group communication:
  - Authorization: Which devices belong to which group
  - Key distribution: Allow authorized devices to send messages
  - Group communication: Use symmetric keys for authentication