Sicher wolkenlos

Muss das wirklich ins Internet?

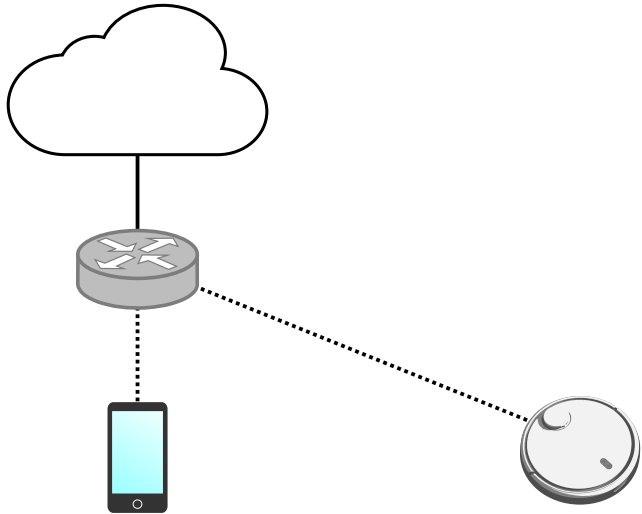
Christian Amsüss <chrysn@fsfe.org>

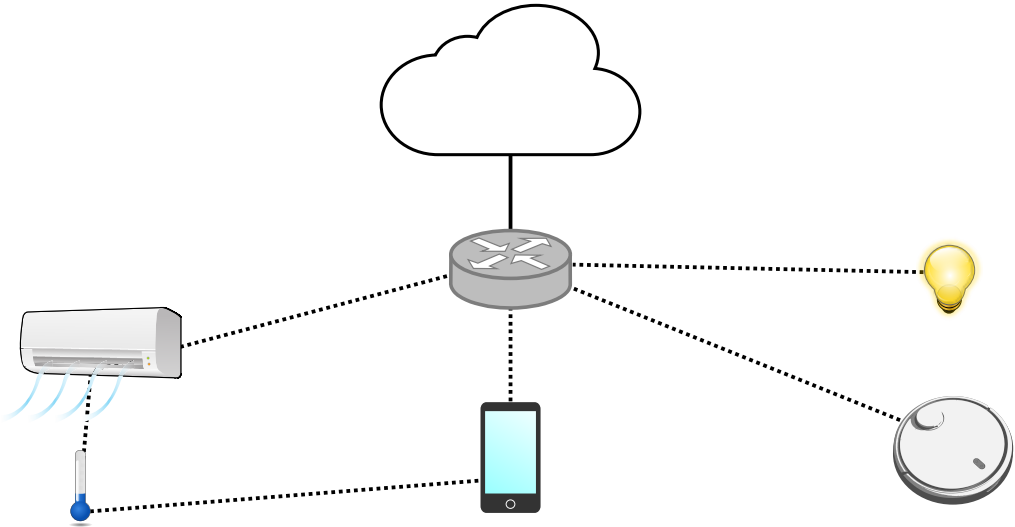
PrivacyWeek 2020

Problemstellung
- Fallbeispiele
- Fokus & Terminologie
- Komponenten der Cloudkommunikation

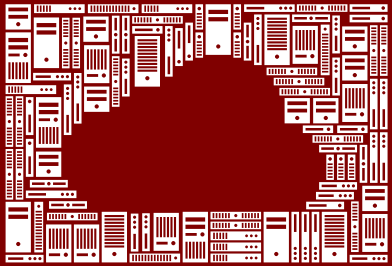
Grundbausteine
- CoAP – Constrained Application Protocol
- CBOR – Concise Binary Object Representation
- COSE – CBOR Object Signing and Encryption

Komponenten für dezentralen Betrieb
- SUIT – Software Updateds for Internet of Things
- OSCORE – Object Security for Constrained RESTful Environments
- ACE – Authentication and Authorization in Constrained Environments



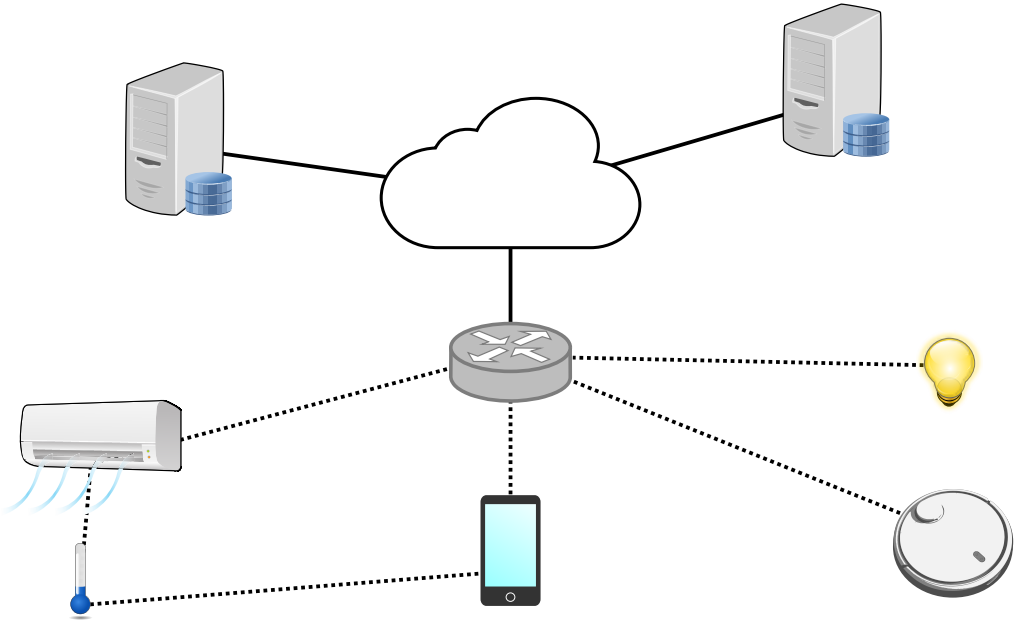


There is NO CLOUD, just

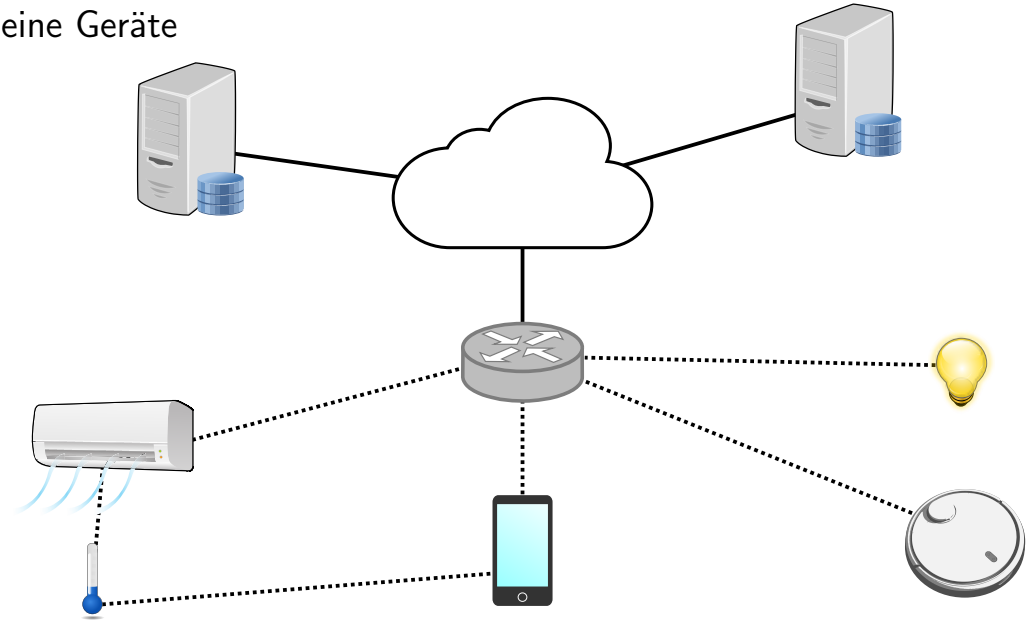


other people's computers

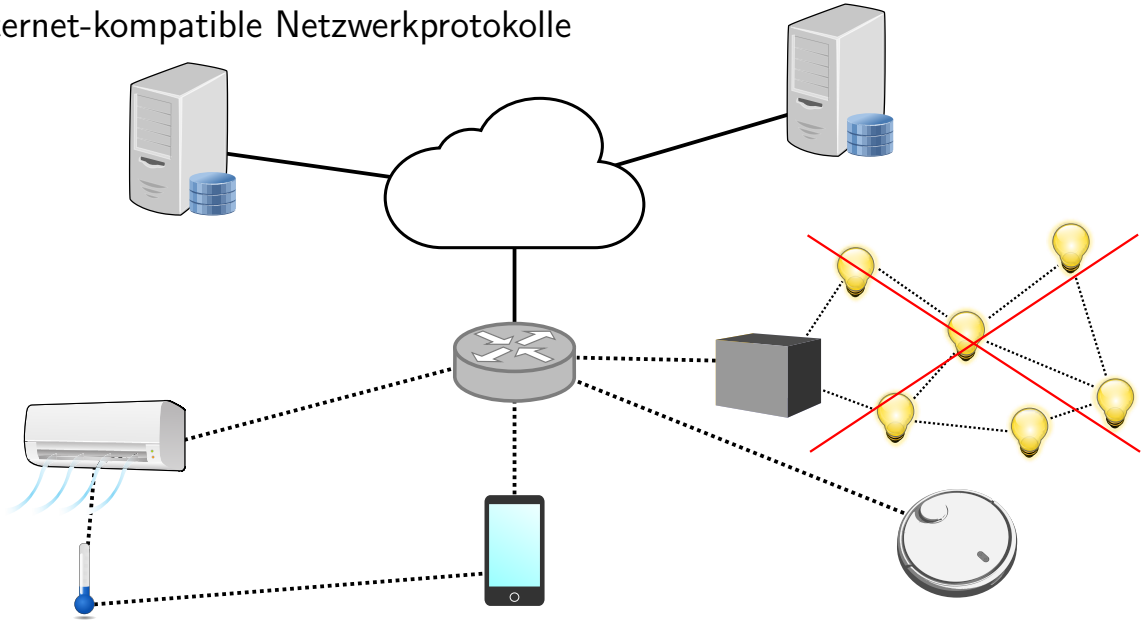
fsfe.org



Kleine Geräte



Internet-kompatible Netzwerkprotokolle



Was tut es mit der Cloud?

- Sicherheit

Was tut es mit der Cloud?

- Sicherheit

- Firmware-Updates
- Rendevouz-Punkt
- Umwegkommunikation
- Benutzerverwaltung
- Datum / Uhrzeit

Was tut es mit der Cloud?

- Sicherheit

- Firmware-Updates
- Rendevouz-Punkt
- Umwegkommunikation
- Benutzerverwaltung
- Datum / Uhrzeit

- Analyse aggregierter Daten
- Reaktionen auf Daten aus dem Internet
- EULAs

Warum?

- Ausfallsicherheit
- Digitale Souveränität
- Datensparsamkeit

Grundbausteine. . .

CBOR Object Signing and Encryption

Concise Binary Object Representation

Constrained Application Protocol

User Datagram Protocol

Internet Protocol

. . . in Analogie zum Web

CoAP

CBOR Object Signing and Encryption

Concise Binary Object Representation

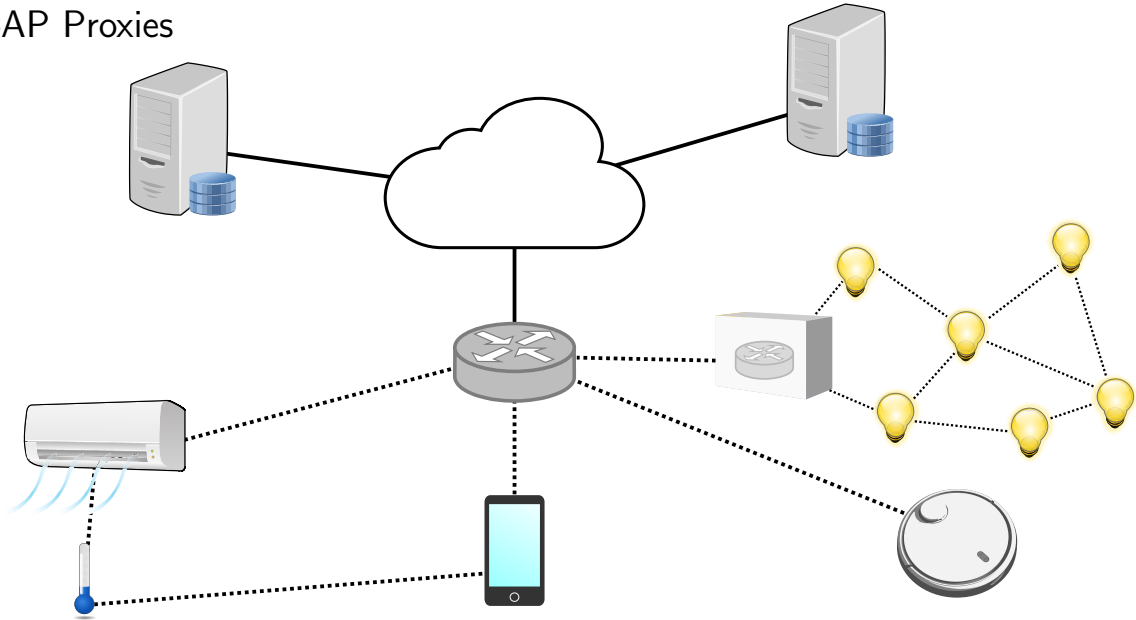
Constrained Application Protocol

User Datagram Protocol

Internet Protocol

Referenz: RFC7252 Implementierungen: > 100 Level: Proposed Standard

CoAP Proxies



CBOR

CBOR Object Signing and Encryption

Concise Binary Object Representation

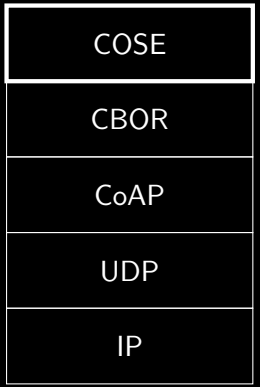
Constrained Application Protocol

User Datagram Protocol

Internet Protocol

Referenz: RFC7049 Implementierungen: > 100 Level: Proposed Standard

COSE



CBOR Object Signing and Encryption

Concise Binary Object Representation

Constrained Application Protocol

User Datagram Protocol

Internet Protocol

Referenz: RFC8152 Implementierungen: > 10[1] Level: Proposed Standard

[1] Darunter die gängigen Web-Browser

Problemstellung
- Fallbeispiele
- Fokus & Terminologie
- Komponenten der Cloudkommunikation

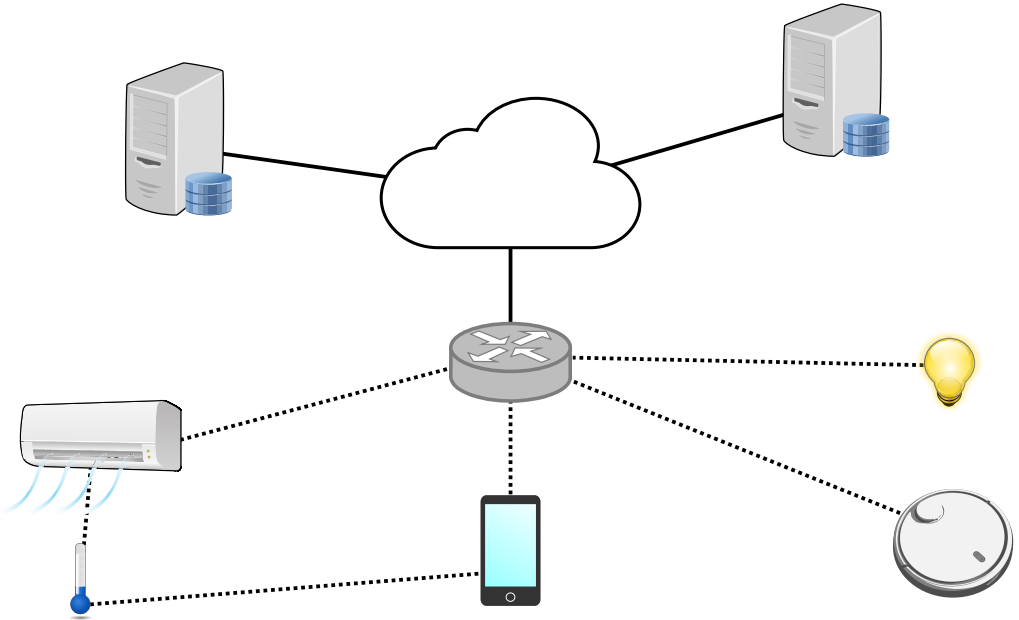
Grundbausteine
- CoAP – Constrained Application Protocol
- CBOR – Concise Binary Object Representation
- COSE – CBOR Object Signing and Encryption

Komponenten für dezentralen Betrieb
- SUIT – Software Updateds for Internet of Things
- OSCORE – Object Security for Constrained RESTful Environments
- ACE – Authentication and Authorization in Constrained Environments

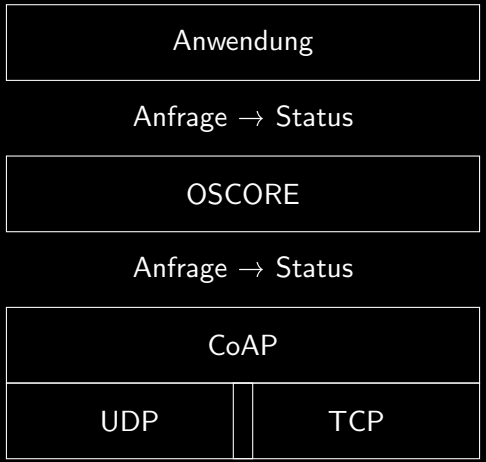
SUIT – Software Updateds for Internet of Things

- Architektur und Datenformat
- Transportunabhängig
- In CBOR ausgedrückt, mit COSE gesichert
- Firmware-Autor und Gerätebetreiber können unabhängig voneinander Freigaben erteilen

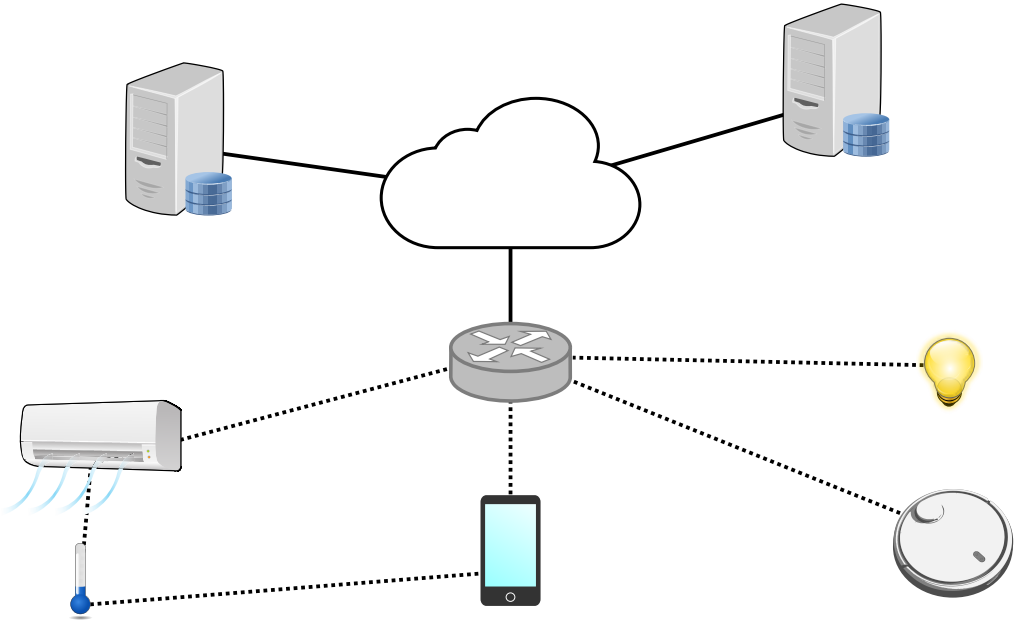
Referenz: I-D.ietf-suit-architecture Implementierungen: > 10 Level: Submitted to IESG



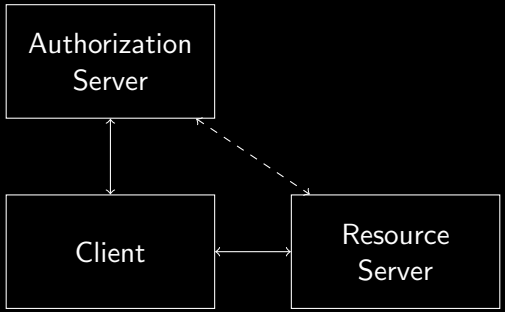
OSCORE – Object Security for Constrained RESTful Environments



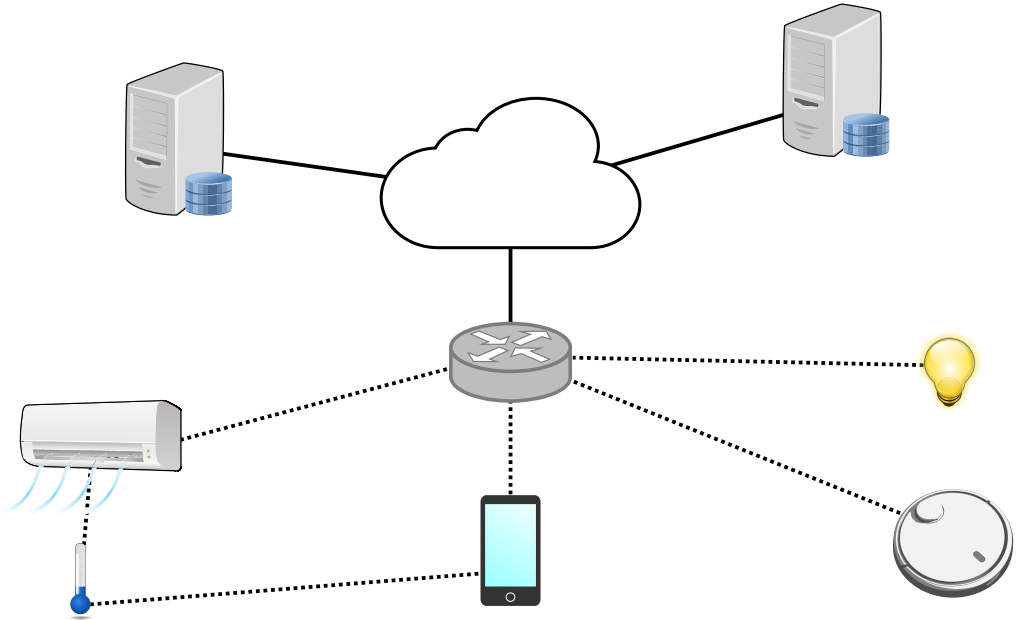
Referenz: RFC8613 Implementierungen: > 10 Level: Proposed Standard



ACE – Authentication and Authorization in Constrained Environments



Referenz: I-D.ietf-ace-oscore-profile Implementierungen: > 10 Level: Submitted to IESG



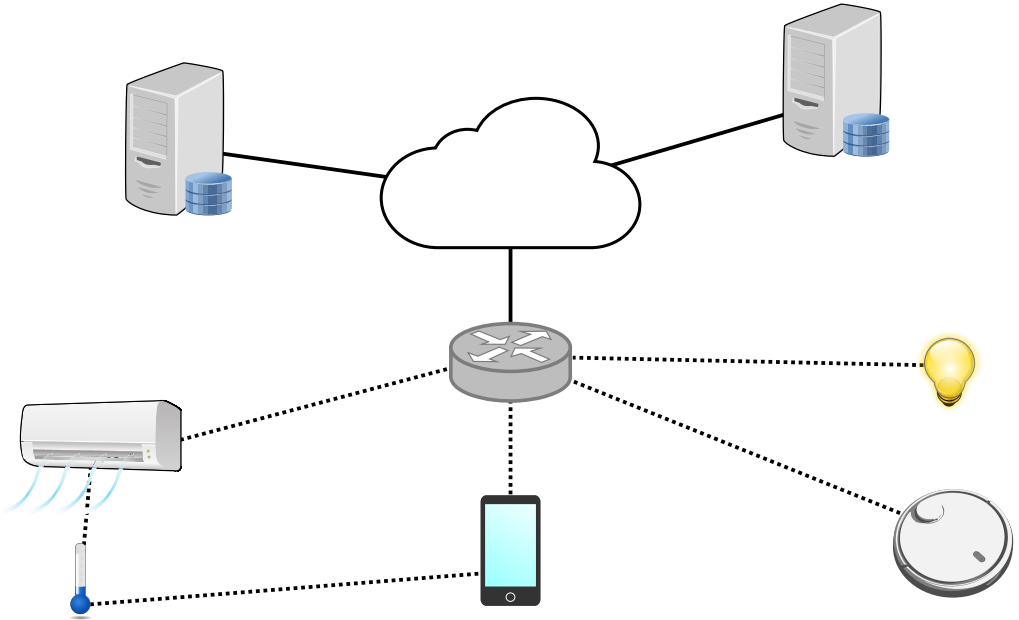
Zurück zu den Anforderungen

- Firmware-Updates
- Rendevouz-Punkt
- Umwegkommunikation
- Benutzerverwaltung
- Datum / Uhrzeit

IoT ohne Onlinezwang ist möglich – fordert das ein!

Folien mit Links auf `https://fahrplan.privacyweek.at/pw20/talk/RQZQGA/`

Christian Amsüss
<chrysn@fsfe.org>



Bausteine

SUIT

OSCORE

ACE

Bildquellen

- „There is no cloud“: Markus Meier, CC-BY-SA 4.0
- „Vacuum robot“: Popey900, copyrighted free use
- „Handy“: FX13, CC-0 1.0
- „Router“: cyberscooty, CC-0 1.0
- „Glühbirne“: jaschon, CC-0 1.0
- „Thermometer“: gnokii, CC-0 1.0
- „Lüftungseinheit“: Juhele, CC-0 1.0

Quelltext der Präsentation ist im PDF eingebettet und unter CC-BY-SA lizenziert.