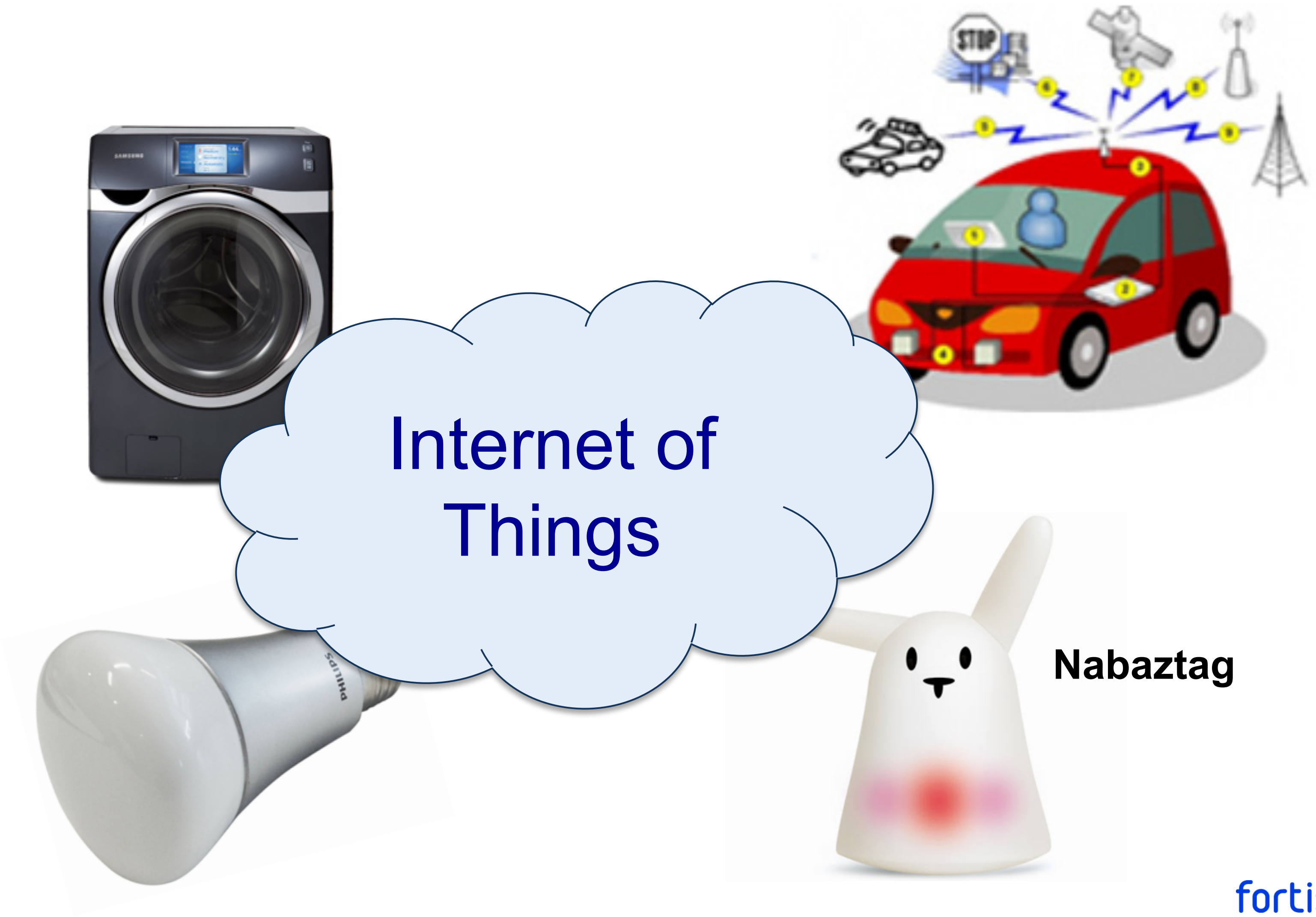
Towards Trusted Apps for the Internet of Things

Christian Prehofer

fortiss GmbH
An-Institut Technische Universität München

Internet of Things – Motivation



Internet of Things

Nabaztag

Contents

- Internet of Things and mobile Apps
- From Mobile IoT Apps to Apps for Things
- Trusted Apps Project

Mobile Apps and the Internet of Things

- Currently, many „smart“ IoT device are used from a **mobile app**

- Examples
  - TV
  - Kitchen devices
  - Lights
  - Cars
  - ...

- For each device, we get an App like a **remote control**
- Simple way to outsource the UI

http://www.wsj.de/nachrichten/SB11401573521024413408604580290843167502192

Mobile Apps for the IoT – Some Views

„Proprietary Apps Will Halt IoT Market Growth“

- Samsung Vice President Dr. Alan Messer:

"Most of those solutions require their app .. in order to use them,“

"app-for-that" model to asking end users to buy a different electric plug and socket for every electric appliance“

http://www.crn.com/news/networking/video/300075925/samsung-proprietary-apps-will-halt-iot-market-growth.htm

http://hackaday.com/2013/07/09/hack-it-in-refrigerator-egg-monitoring/

Example: Download the App for your recipe

- **Example recipe app** – downloaded on demand
- So stellt sich ein traditionsreicher Hausgerätekonzern wie Miele die Zukunft vor: Ein junges Pärchen verfolgt im Fernsehen eine Kochsendung. Die macht ihnen Appetit, und sie beschließen, das Menü nachzukochen. Über eine App ihres Geräteherstellers laden sie das nötige Backprogramm für den Braten herunter, beim Sender gibt es die Zutatenliste im Download. Der Kühlschrank vergleicht und stellt fest, was noch einzukaufen ist. Bestellt wird natürlich auch online, und nach der Lieferung kann es dann losgehen: Zutaten vorbereiten, alles kleinschneiden und die Gerichte vorbereiten. Den Rest erledigt der Backofen selbstständig

http://www.wsj.de/nachrichten/SB11401573521024413408604580290843167502192

So what about your recipe App ...

- So, take the **recipe App** example ...

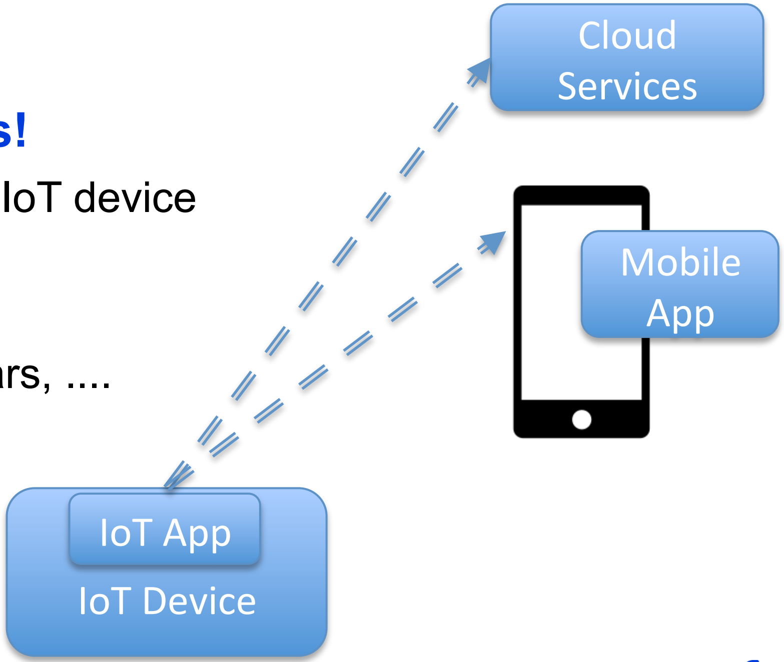
- **What happens** with your food if ...
  - you leave the house?
  - your phone crashes?
  - there is a virus on your phone?

- Just consider **malicous Apps:**
  - In a dataset of 22500+ Android apps, 26% of their samples are identified as malicious
    - A. Gorla et al., Checking App Behavior Against App Descriptions

From mobile Apps to (trusted) Apps for Things

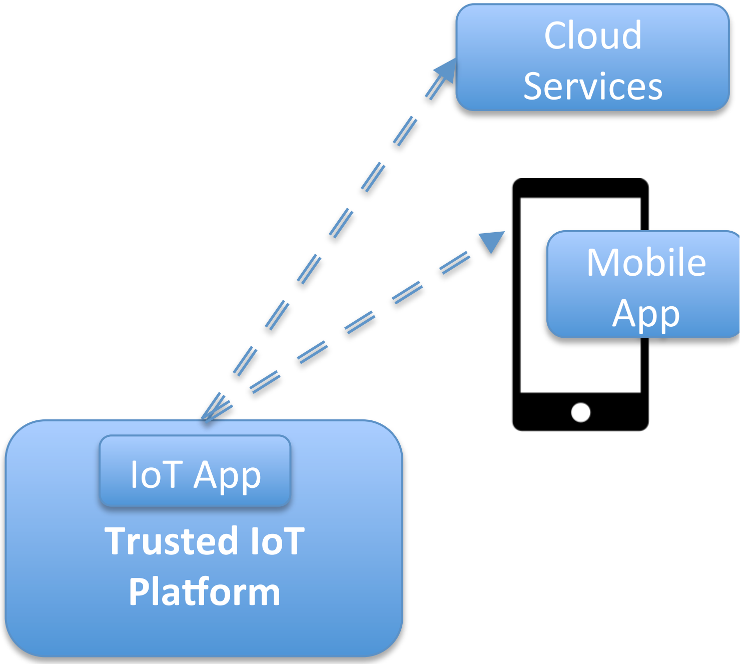
- Main **requirements**
  - Apps for (critical) devices need to be **highly trusted**
    - Apps and open interfaces to devices create security risks
  - Apps must not **loose connection** to the IoT device
    - Loss of connection is loss of control
  - Usability, easy of deployment, ...

- Approach here: put **apps on things!**
  - Apps should be on the „thing“ – the IoT device
    - Maybe on (home) gateway
    - Mobile Apps in addition to this
  - Already happening for Cameras, Cars, ...



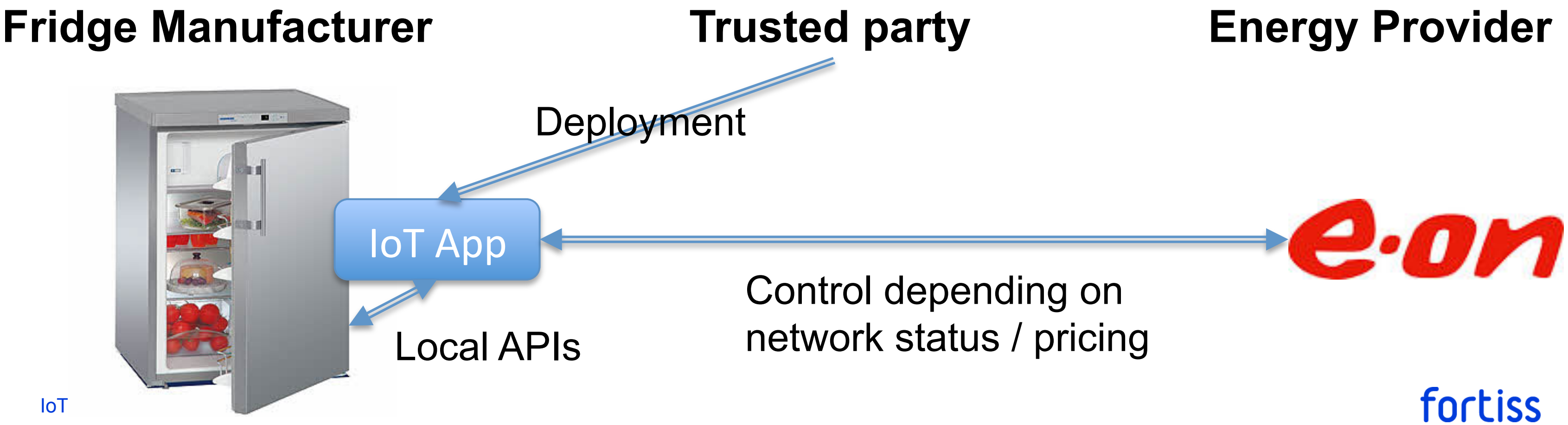
Plattform for Apps for Things

- **We need a platform for highly trusted Apps on IoT devices**
  - No loss of connection
  - Local processing (e.g. important for multimedia processing)
  - Higher security possible (e.g. no man-in-the-middle)
- Challenges for **„real IoT Apps“**
  - IoT platforms not designed for „platform security“
    - Simple operating systems/HW
    - No virtualization or even memory protection
  - Limited UI and configuration
- **Current work** at fortiss on
  - Secure Apps for Contiki OS (not focus today)
  - Trusted Application Platform **TAPPS**
    - See next slides



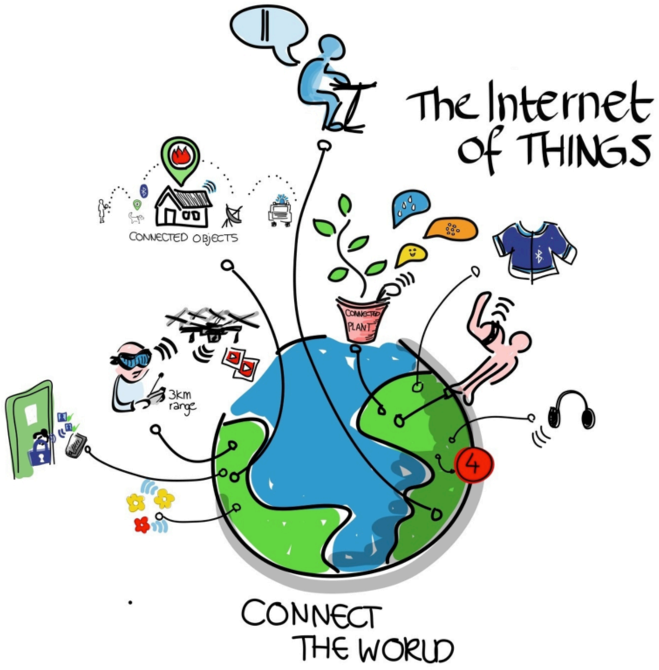
Smart Grid Example: Energy Control for a Fridge

- **Motivation**: Use a fridge for energy storage
  - e.g. introduce low, normal and high modes wrt energy consumption
- **Problem**: Large number of manufacturers and energy providers
  - Large number of business relationships & target devices
- **App-based Approach**
  1. Fridge manufacturer provides App platform
  2. Energy provider provides app to control energy
  3. App is checked by some trusted party (may be (1))



IoT Service Ecosytems

- **Open eco-systems** can spark innovation
  - Examples: Windows, mobile apps (iPhone, Android), SAP, ...
  - Secure R&D investment
  - Enables new value chains and scalable revenue models
- IoT connects to the Internet with **fast innovation cycles**
  - Requires quick innovation and update cycles
- **Large number** of different devices
- Closed & vertical systems for IoT **hinder IoT adoption**
  - Slow development and deployment
  - Solutions specific to platforms and not portable



*Trusted **Apps** for open CPS (TAPPS)*

- **Goal: open platform for trusted Apps**
  - Adding features by downloading apps
  - Apps may interfere with safety critical functions
- **Main innovation**: Trusted App Platform
  - Incl. trusted HW, OS, Tool Chain, App Store
- TAPPS partners

TAPPS

EU Horizon2020 Project
tapps-project.eu

fortiss

ST life.augmented

TTTech

Virtual Open Systems

actility

FCSR Fondazione Centro San Raffaele

Technological Education Institution of Crete

CRP

Ospedale San Raffaele

Partners of TAPPS

fortiss

life.augmented

TTTech

Virtual Open Systems

actility
Making Things Smart

FCSR
Fondazione
Centro San Raffaele

TECHNOLOGICAL
EDUCATION
INSTITUTION
OF CRETE

CRP

OSPEDALE
SAN RAFFAELE

(Third party)

Contact

Presenter name // Organisation

Email – (phone number)

TAPPS
Trusted **Apps** for open CPSs

Co-funded by the Horizon 2020
Framework Programme of the European
Union under grant agreement no 645119

TAPPS Motivation

- Trend towards **open systems**, which can be extended during operation.
  - Add features by downloading apps
  - Apps may interact or interfere with safety critical functions

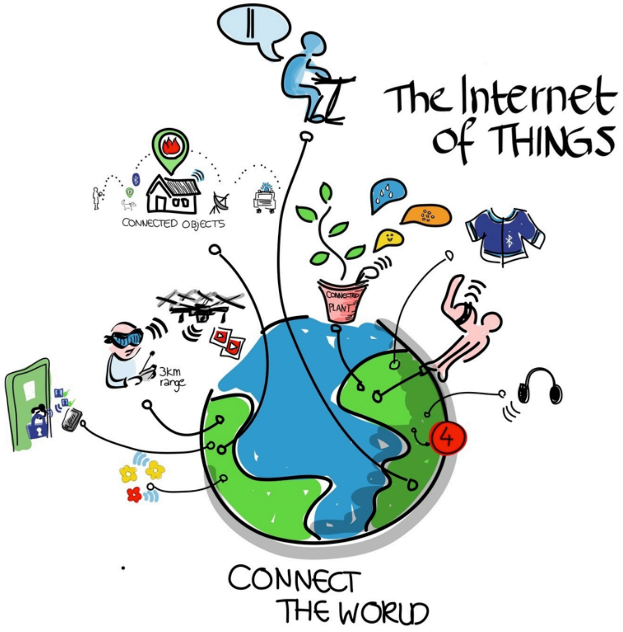
- Not possible today due to **security and safety**

TAPPS: Trusted Apps Eco-Systems

- **Apps in vehicles** or other „critical“ devices to add new functionality
  - To add new features and customization
  - Apps as a key differentiating feature

- Goal is build an **eco-system of apps**
  - Invite 3rd parties to innovate on top of existing plaforms
    - E.g. open car as a SW platform
  - Also considering health and other domains

- Main challenge is **trust**
  - Trust includes security, safety, management and cor
  - A main challenge is to ensure safety of the devices



fortiss

Apps in Smart Devices (Vehicles, Health)

- **Categories of Apps** (in case of vehicles)
  1. Pure **infotainment**, external services
     - Safety relevance is low
  2. Apps which **access internal information**
     - E.g. address book, sensors, location, ...
     - Privacy issues, little safety issues
  3. Integrated Apps which **modify internals**
     - E.g. customize vehicle dynamics (traction, esp, ...) based on weather conditions
     - E.g. customize assistance systems

- Focus here is on class (3): **apps which have access to internal APIs**
  - High demands on safety and security.
  - Requires a dedicated, secure execution environement
    - Note: may be complemented by an app for less critical tasks (e.g. UI, external interfaces) in a less trusted execution environment

Safety and Security Issues for Apps

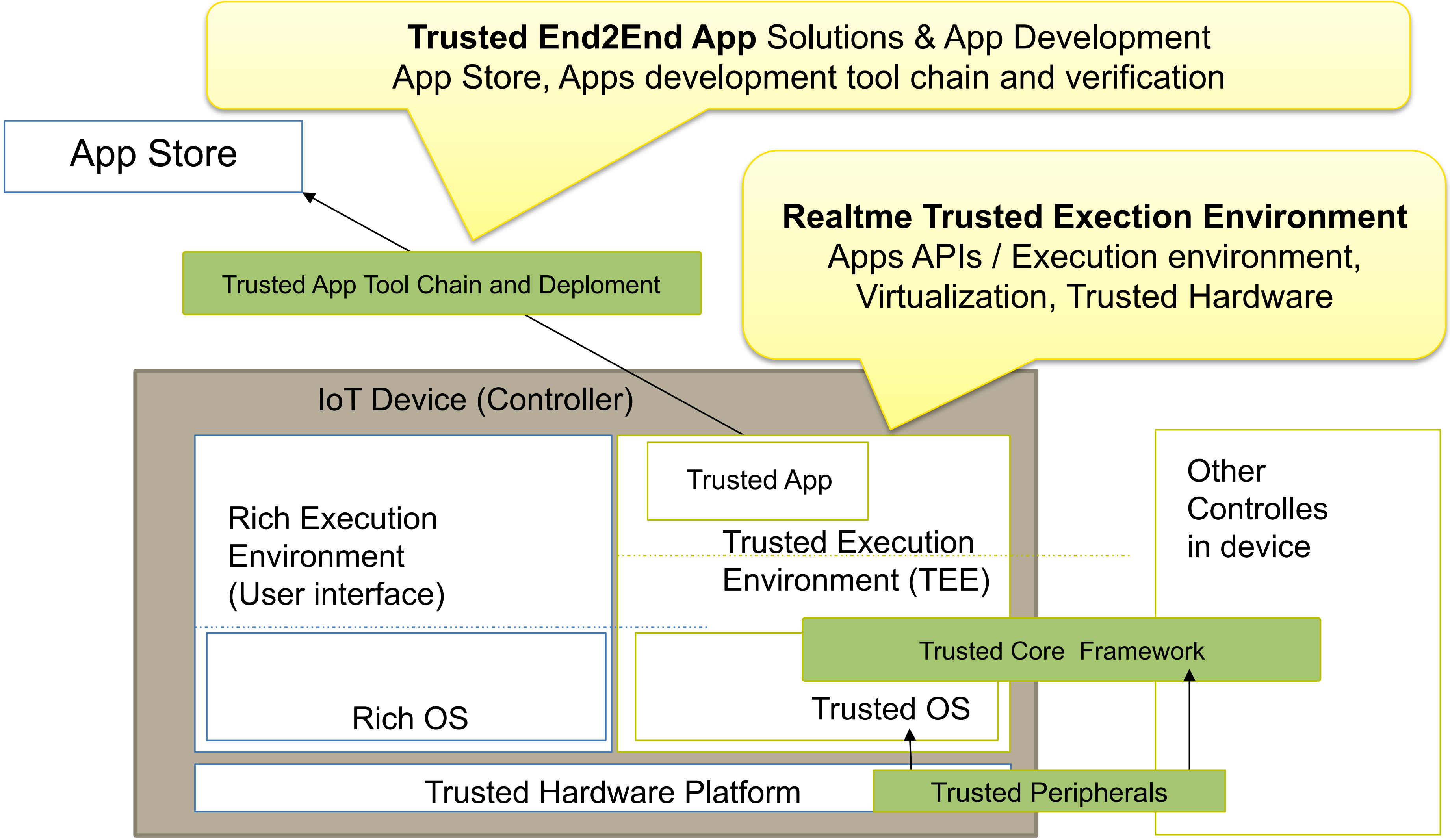
- **Resource issues:** Apps may use considerable system resources
    - Other apps and functions may suffer
    - Concerns network, CPU and others (e.g. HW interfaces, storage, ..)
    - Need of virtualization of resources
        - Needs to go beyond single ECU – include NW etc
        - Management of these resources is needed
- **Fine grained access control**
    - E.g. application may get the position once or continously
    - E.g. app may get one entry from the phone book, but not the full phone book
- **Safety critical 3rd party apps** may need verification
    - Simple testing or static checking not always sufficient
    - Need proper verification – e.g. by model checking

TAPPS: Trusted Execution Environment

- **Challenge: Realtime Trusted Execution Environment (TEE)** for highly-trusted Apps.

- Main Approach: **Multiple layers of security**
  1. **Trusted hardware** with security mechanisms
  2. **Computing and network virtualization**
  3. **Fine-grained access control** to resources of the smart device to ensure safety and privacy.
  4. **Verified Apps** to ensure correct and secure behavior.

TAPPS Approach and main Goals


Trusted End2End App Solutions & App Development
App Store, Apps development tool chain and verification
App Store
Trusted App Tool Chain and Deploment
Realtme Trusted Exection Environment
Apps APIs / Execution environment,
Virtualization, Trusted Hardware
IoT Device (Controller)
Rich Execution Environment (User interface)
Rich OS
Trusted App
Trusted Execution Environment (TEE)
Trusted Core Framework
Trusted OS
Other Controlles in device
Trusted Hardware Platform
Trusted Peripherals

fortiss

End-to-end Solution

End-to-end solution for development and deployment of trusted Apps

- An **application store** for management of CPS Apps and for deployment, supporting both the rich execution environment and the separate TEE.
- A **model-based development tool chain** for designing and implementing trusted apps including APIs and verification tools.

Research challenges

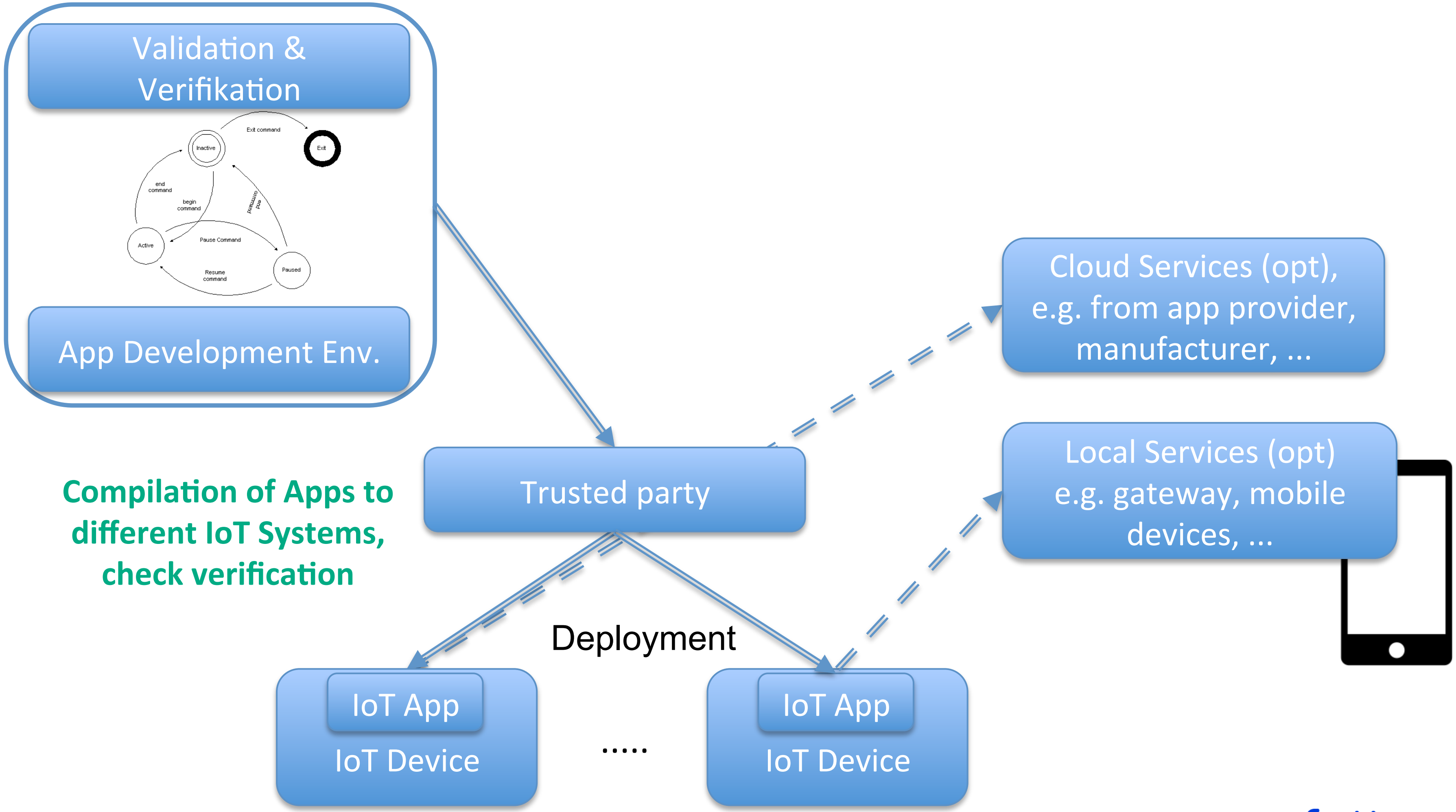
- **Integrated management of security**
  - User profile, credentials, API access rights, device capabilities throughout the complete solution, including App Store, deployment and Apps configuration and access control.

- **Tight integration of HW security with computing and network virtualization**, including real-time support and APIs for apps.

- **Tool support for the development of apps** in a small, trusted execution environment.

- **Verification of trusted apps** by new verification tools.

TAPPS High-level System Architecture



Validation & Verifikation

App Development Env.

Compilation of Apps to different IoT Systems, check verification

Trusted party

Cloud Services (opt), e.g. from app provider, manufacturer, ...

Local Services (opt) e.g. gateway, mobile devices, ...

Deployment

IoT App

IoT Device

.....

IoT App

IoT Device

Validation Goals

- Validated in health and automotive application domains

Summary

- Many **great IoT applications**, but also too many vertical silos
- **Trusted apps** can be the basis for open, flexible IoT ecosystems
  - Trust as needed for sensitive and/or safety-relevant applications
- Need an open platform for **trusted apps on IoT devices**
- **TAPPS project** works on a trusted platform for Apps
  - Multiple layers of security (HW, virtualization, APIs, verification)
  - End-to-end solution for deployment and apps management