Security Challenges in IoT

UN/CEFACT Conference –
IoT for Trade Facilitation on Apr 24th 2018

Dr. Josef Haid
Lead Principal, Infineon Technologies AG

The definition of IoT

"A world where **physical objects** are seamlessly **integrated** into the **information network**." SAP

IoT security is a focus topic in the industry

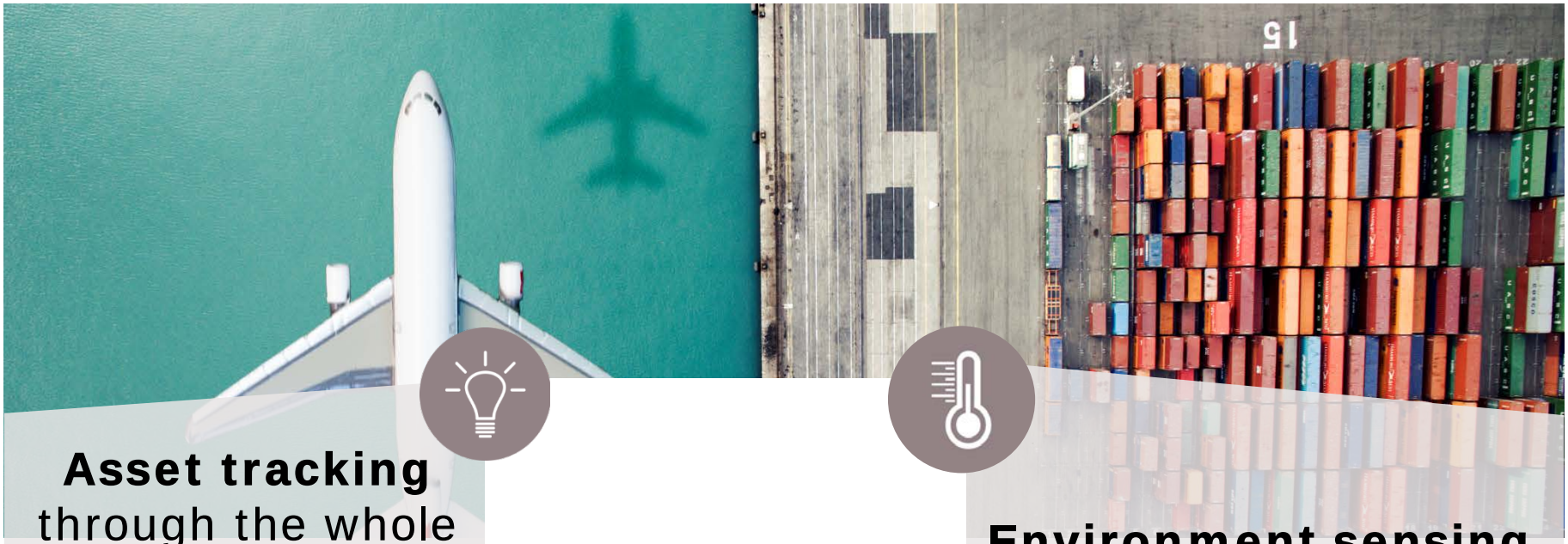
30 billion
devices by 2020
ABI

547 million
IoT security spending
in 2018
Gartner

The IoT is expected to create significant value across industries

IoT security needs to protect this value

IoT devices used to support reliable and trusted manufacturing and delivery of goods



Asset tracking through the whole manufacturing and delivering cycle

Fleet manage-ment to optimize transportation resources

Environment sensing to monitor sensitive goods to avoid damage or loss

Applications are increasingly exploiting the potential of IoT devices

Applications

Smart Factory/ Industry 4.0

Smart Home

Connected cars

Use cases

Environmental monitoring and sensing (temperature, pressure, speed…)

Remote control of actuators (motors, lights, machines, supplies…)

Cloud-based services (automated building control, traffic control…)

Security concerns customers

IoT Abstract Architecture - Conceptual Layers

Gather data; analyze and send commands

Server

Reliably convey data and commands

Network

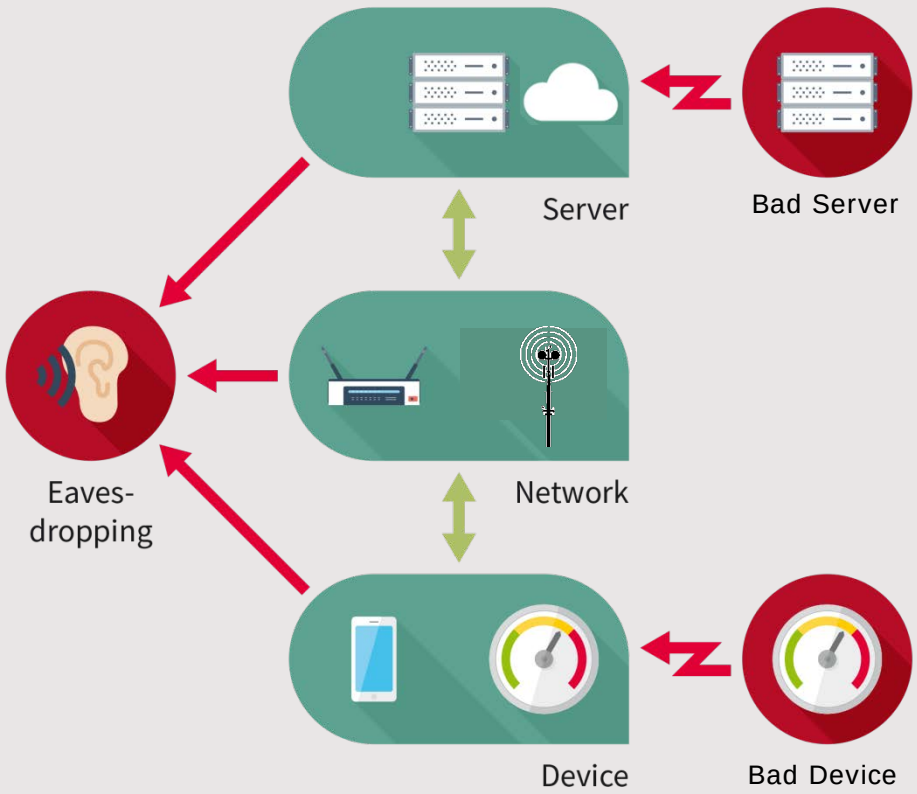
Send and receive data and commands

Device

Each Layer can be Attacked

Security threats for IoT

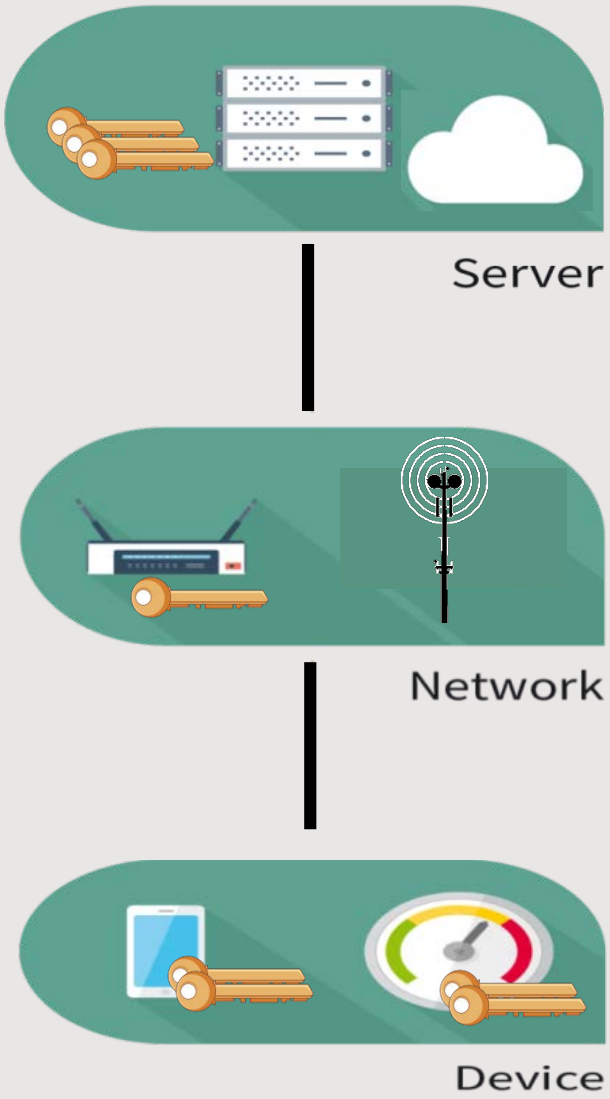
An **Eavesdropper** listening in on data or commands can reveal confidential information about the operation of the infrastructure.



A **Bad Server** sending incorrect commands can be used to trigger unplanned events, to send some physical resource (water, oil, electricity, etc.) to an unplanned destination, and so forth.

A **Bad Device** injecting fake measurements can disrupt the control processes and cause them to react inappropriately or dangerously, or can be used to mask physical attacks.

Three effective measures in IoT Security

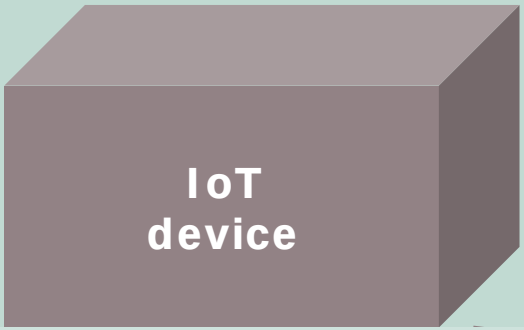


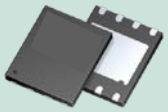
Authentication to establish a trusted connection between device and service

Secured communication to protect from eavesdropping

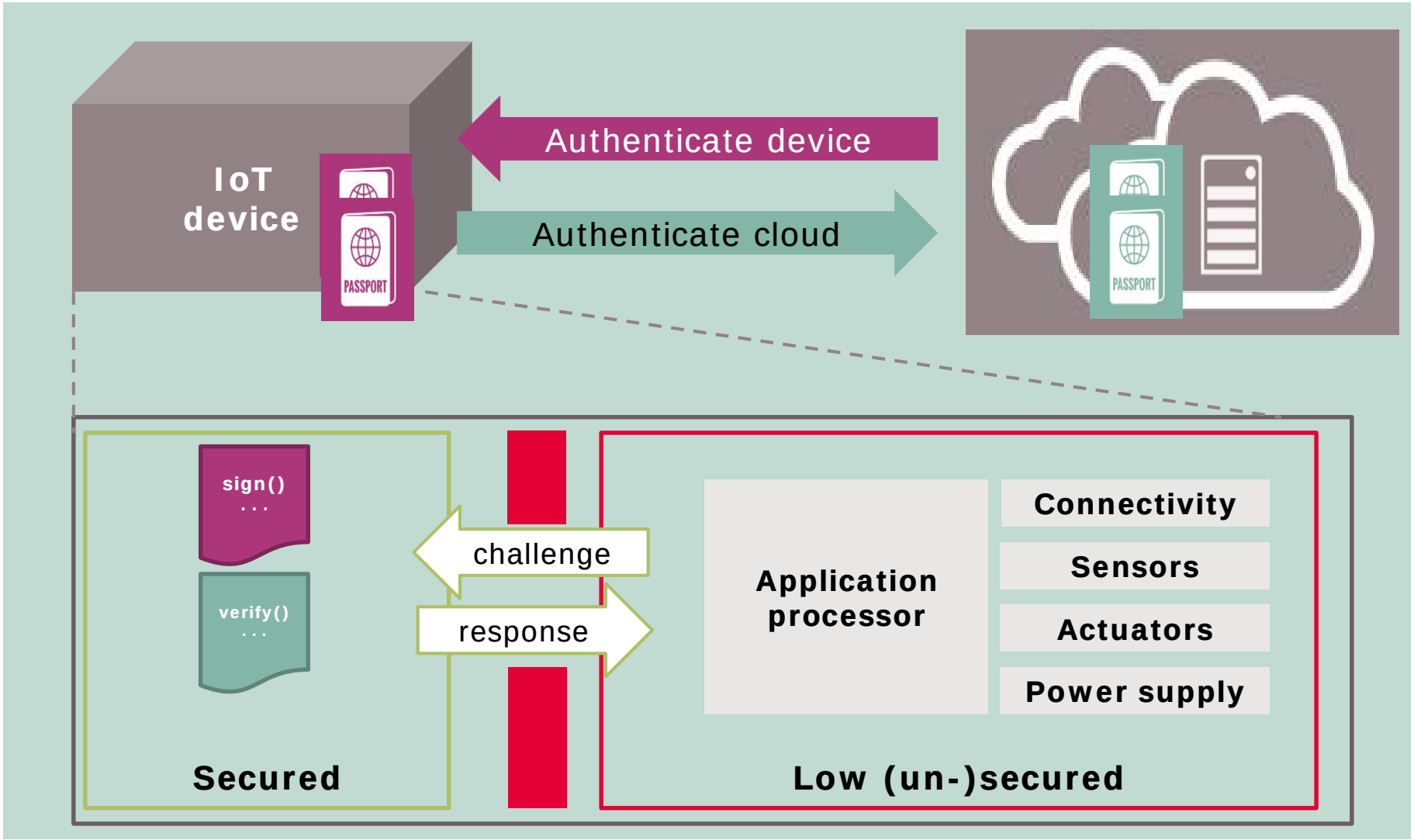
Secured Firmware Update to reduce risk of corrupted software to be uploaded

Protecting IoT edge device architectures is essential – Using **Hardware Root of Trusts**

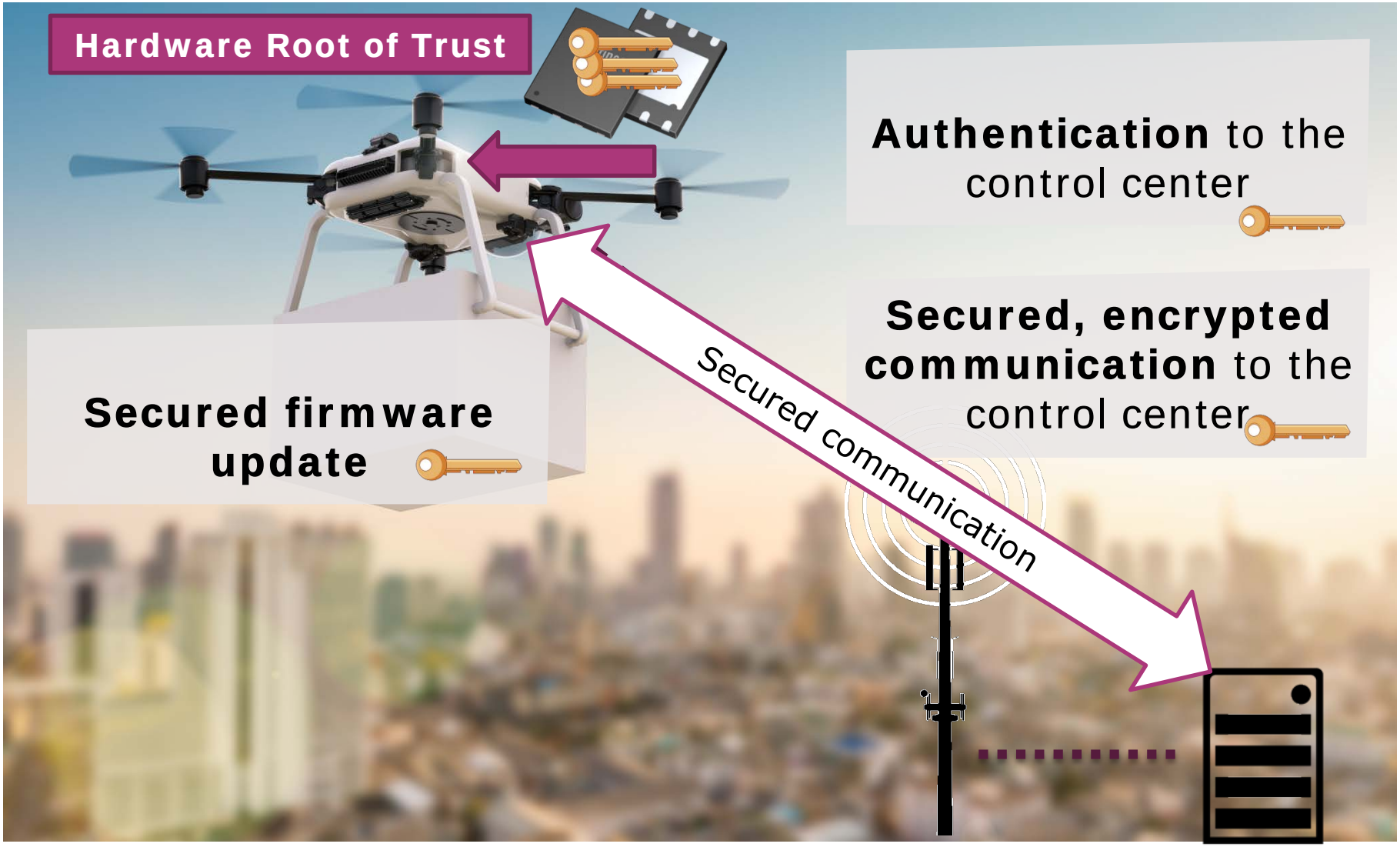




Authentication – identities must be protected in **Hardware Root of Trusts**



Secured IoT Devices can revolutionize industries



Hardware Root of Trust adds value by protecting business and enabling growth

Implementation of **reliable, efficient and trusted supply chains**

Implementation of **sustainable and secured IoT-systems**

Part of your life. Part of tomorrow.

Infineon