The easy way to secure smart air conditioners

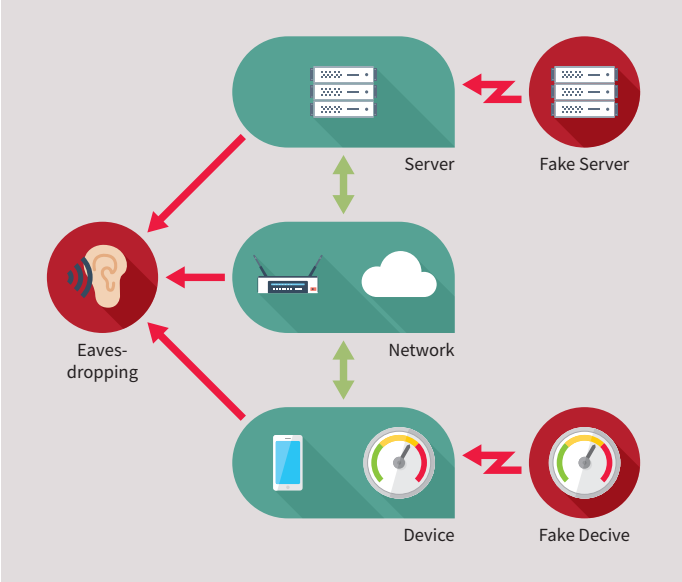
www.infineon.com

With the increase in network connectivity for smart air conditioners (such as WIFI or Bluetooth), smart air conditioners are exposing a greater surface to attacks.
For example, we have seen how the vulnerability of the WIFI protocols was compromised by the KRACK attack. Serious weaknesses were discovered within the WPA2 protocol which secures all modern protected WiFi networks.
In another example, the BlueBourne attack exploits weaknesses in Bluetooth protocol to gain full access to these devices to extract sensitive information.
Smart devices that were deployed with weak or default passwords allow adversaries to inject malware and turning the devices into a Botnet or locking down a commercial air conditioner system using Ransomware for monetary gains.
This security guide for smart air conditioners will explain why hardware based security is the right answer to security vulnerabilities at smart air conditioner systems and how easy it is to implement it.

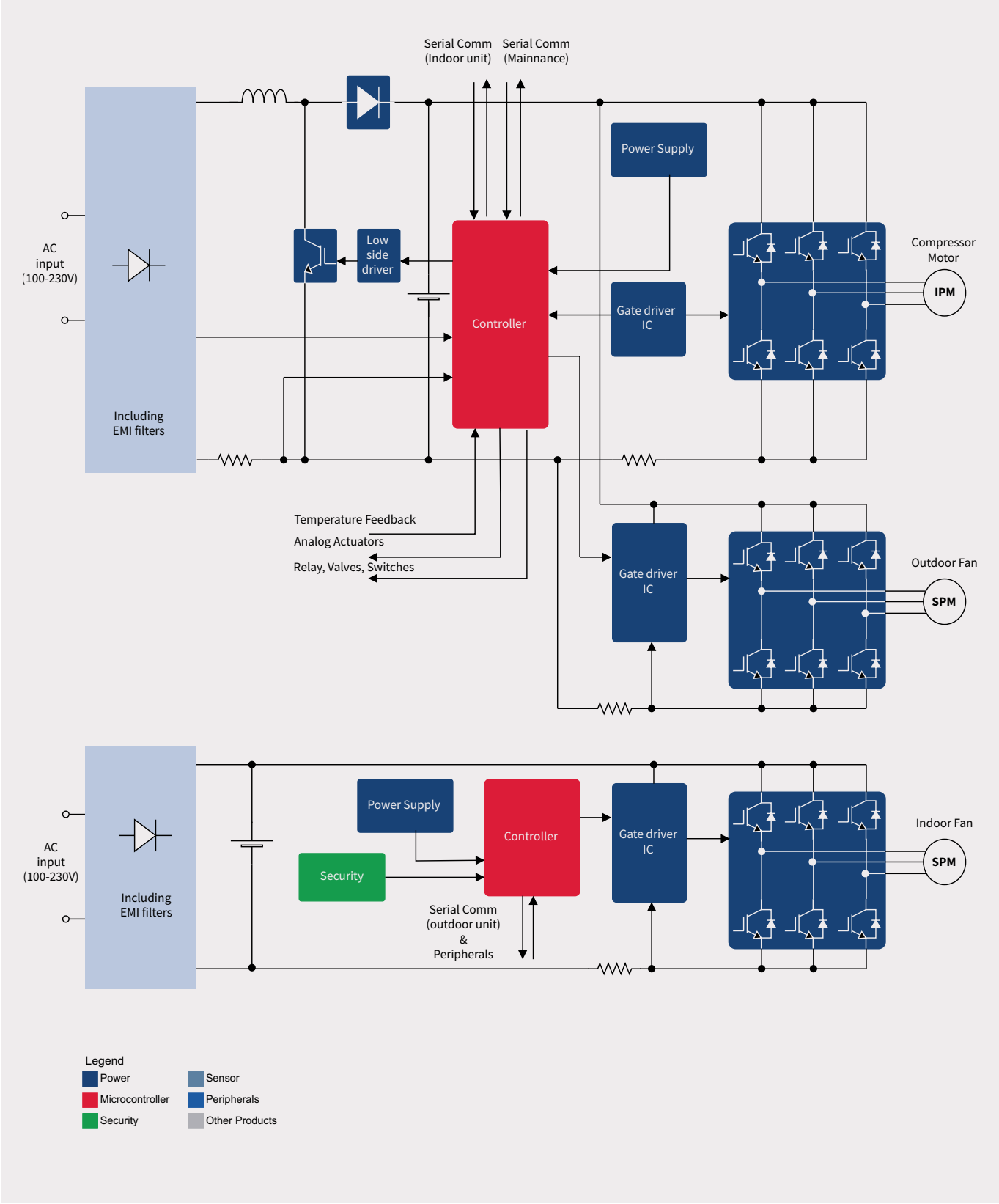
Security concerns that need to be addressed

In order to design a secured smart air conditioner, there are a few fundamental security objectives that need to be achieved:

- Identity protection against fake devices: How can I verify my device identity using cryptographic means for security?
- Protection against eavesdropping: How do I protect my data privacy from eavesdropping and theft?
- Protection against the manipulation of the data: How do I prevent my data (e.g usage details, configuration parameters, applications etc.) from unauthorized modification?
- Protection against illegal update of firmware or software: How do I prevent malicious firmware from being injected into the device?



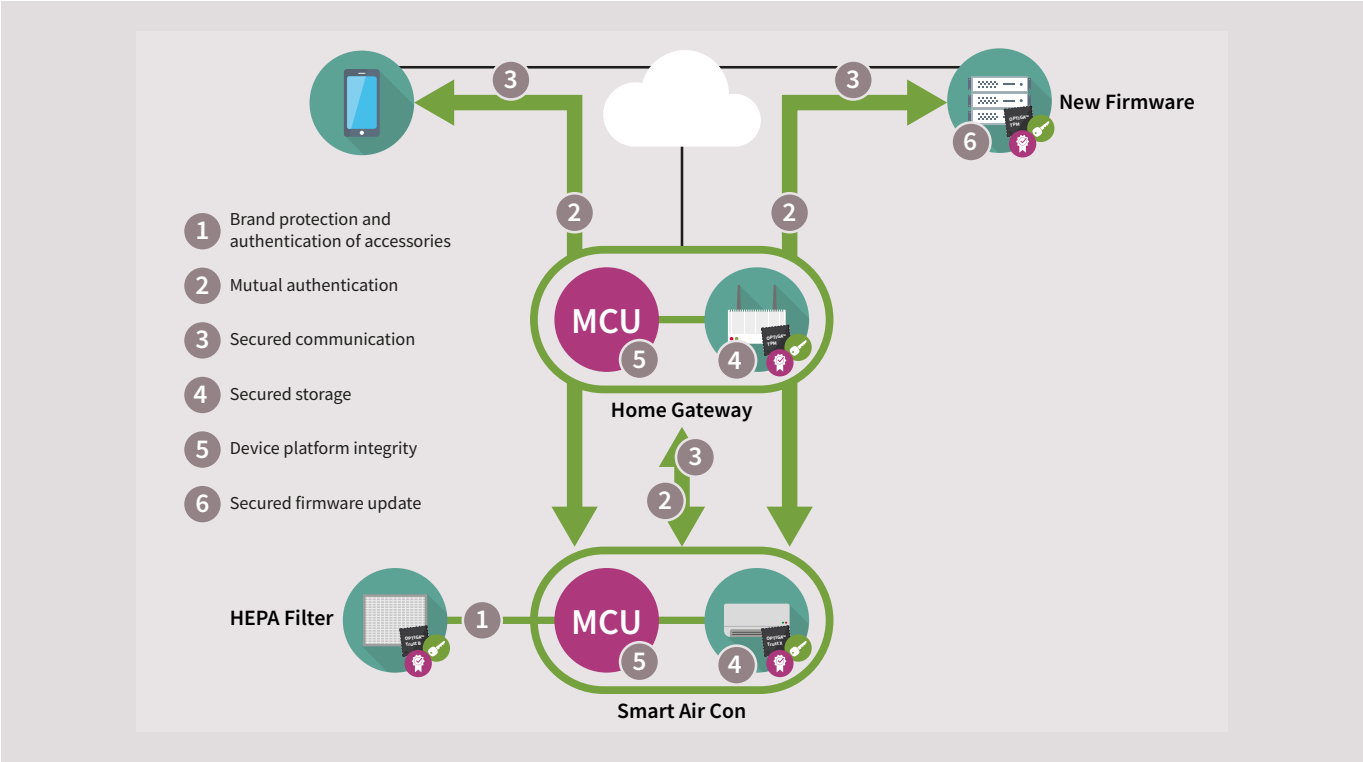
How OPTIGA™ Trust Anchor for smart air conditioners work and how easy it is to get implemented



In order to get confidential data such as cryptographic keys, device certificates or parameters secured, you only need to easily store this data on the OPTIGA™ Trust Anchor. As you can see in the picture above the OPTIGA™ Trust Anchor is easily incorporated into the smart air conditioner design adjacent to the Central Control Unit.

Use cases for air conditioners and how to get started:

The OPTIGA™ Trust Anchor comes pre-provisioned with the first key pair and certificates from Infineon Common Criteria certified factory. This eliminates the need for customers to perform first key pair injection which can be costly as it requires secured premises. The following security use cases can easily be implemented with the OPTIGA™ Trust Anchor:



Use Case for OPTIGA™ Trust family	Description
Brand protection and authentication of accessories	OPTIGA™ Trust B can be used in smart air conditioner accessories/consumables (such as HEPA filters) to verify that genuine parts are used.
Mutual authentication	OPTIGA™ Trust X (which secures the secret keys and certificates) can be used to perform mutual authentication with clouds and OEM servers. This helps the smart air conditioning manufacturers to securely identify the air conditioning device that connects to their servers.
Secured communication	OPTIGA™ Trust X can be used to establish secured communication with the cloud and OEM servers.
Secured storage	OPTIGA™ Trust X adopts a Common Criteria EAL6+ certified hardware trust anchor which offers protection against various physical and reverse-engineering attacks. Data stored in the Trust X is protected against various extraction techniques as verified by the Common Criteria certification.
Device platform integrity	OPTIGA™ Trust X can be used to perform platform integrity measurements and checks to verify securely whether the device has been infected by malicious malware for example.
Secured firmware update	OPTIGA™ Trust X can be used to cryptographically verify and perform secured firmware update.

It's easy to get started

A simple way to get started on adding security into smart air conditioners will be to incorporate OPTIGA™ Trust X into the design. Customers can download the support packages from the open source GitHub links below and add security into their design.

a) github.com/Infineon/optiga-trust-x
b) github.com/Infineon/personalize-optiga-trust-x
c) github.com/Infineon/getstarted-optiga-trust-x
d) github.com/Infineon/appnotes-optiga-trust-x
e) github.com/Infineon/mbedtls-optiga-trust-x
f) github.com/Infineon/amazon-freertos-optiga-trust-x

Special support for our distribution partners:

Use our tool:

www.infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-security-solutions/#!myInfineon

Our support material ranges from deeper product information, buyer guide for the different products (within "getting started"), customer presentation material to even trainings on security.

www.infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 03 / 2019