Alibaba Cloud with OPTIGA™ Trust M2 ID2

Securing connectivity to Ali Cloud Link ID^2 with OPTIGA™ Trust M2 ID2

www.infineon.com/optiga-trust-m

Synopsis

As cloud-based services grow in importance, so too does the need for device security and secured connectivity between IoT devices and cloud.

A leading global cloud services provider, Ali Cloud Link ID^2 platform spans IoT devices, the Link ID^2 distribution center, the Link ID^2 authentication center and Internet service.

Reaching beyond software-only protection, hardware-based security adds an additional layer of security to IoT devices. This paper looks at how Infineon's OPTIGA™ Trust M2 ID2 security solution can be integrated into an IoT device to harden device security and protect communication with Alibaba Cloud's IoT platform by combining tamper-resistant hardware with a tailored set of ready-to-use security functions. It further illustrates how OPTIGA™ Trust M2 ID2 simplifies and accelerates the integration process thanks to for support for different host platforms and TLS libraries, also providing ease of use with a host-side library.

Contents

1. Introduction 4

2. Ali Cloud Link ID² infrastructure overview 5

3. Alibaba Cloud IoT security 6

3.1 Ali Cloud Link ID² authentication process 6

4. Hardening security for IoT devices using Infineon OPTIGA™ Trust M2 ID2 7

4.1 Infineon OPTIGA™ Trust M2 ID2 7

4.2 Integration with an Alibaba Cloud connected IoT device 8

4.3 Device enrollment process at Alibaba Cloud IoT 9

4.4 Hardware-based security 9

5. Conclusion 10

6. Glossary 11

7. References 12

1. Introduction

The IoT connects a diverse array of devices with one another or with cloud based services. The ability to exchange data with other devices, services and users is a fundamental requirement for IoT solution providers to develop new use cases and business models.

Today, communication technologies provide connectivity between almost any two places on earth, at ever increasing speeds. The proliferation of cloud based storage and computing infrastructure has led to a multitude of cloud based technology offerings from both, large players such as Alibaba Cloud [1], Amazon, Google, Microsoft, and IBM as well as from many new ventures. At the same time, the availability of hardware and software for embedded connected devices has grown significantly.
Affordable single board computers such as Raspberry Pi or microcontroller platforms such as Arduino empower millions of developers to engineer new applications.

As more devices connect to the Internet, however, they are also becoming the target of deliberate attacks as shown in below picture.

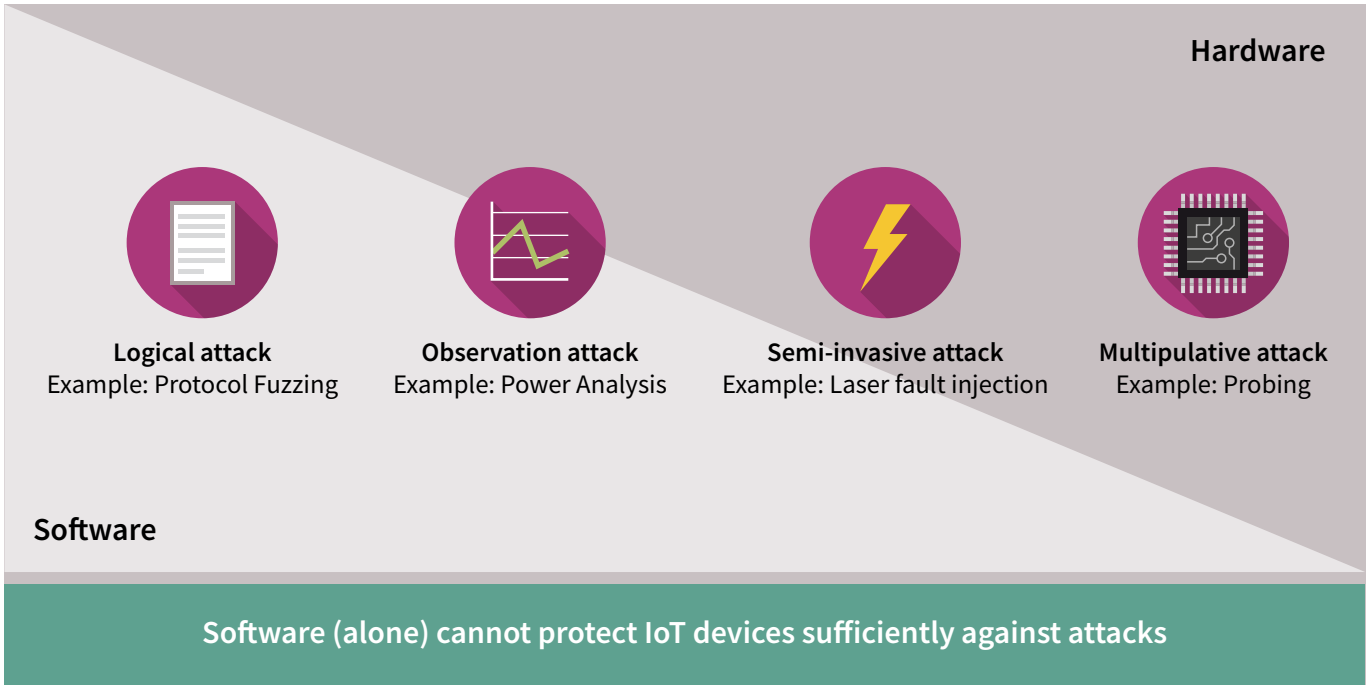


Figure 1: Types of attacks

2. Ali Cloud Link ID² infrastructure overview

Cloud services provide remote infrastructure, services, and solutions on a pay-per-use basis and do not require a large upfront investment. IoT customers can thus benefit from high availability and scalability and focus on their core business.

Ali Cloud Link ID² gives IoT devices a trusted identity. It is based on a unique global security attribute that is protected from being tampered with or forged.

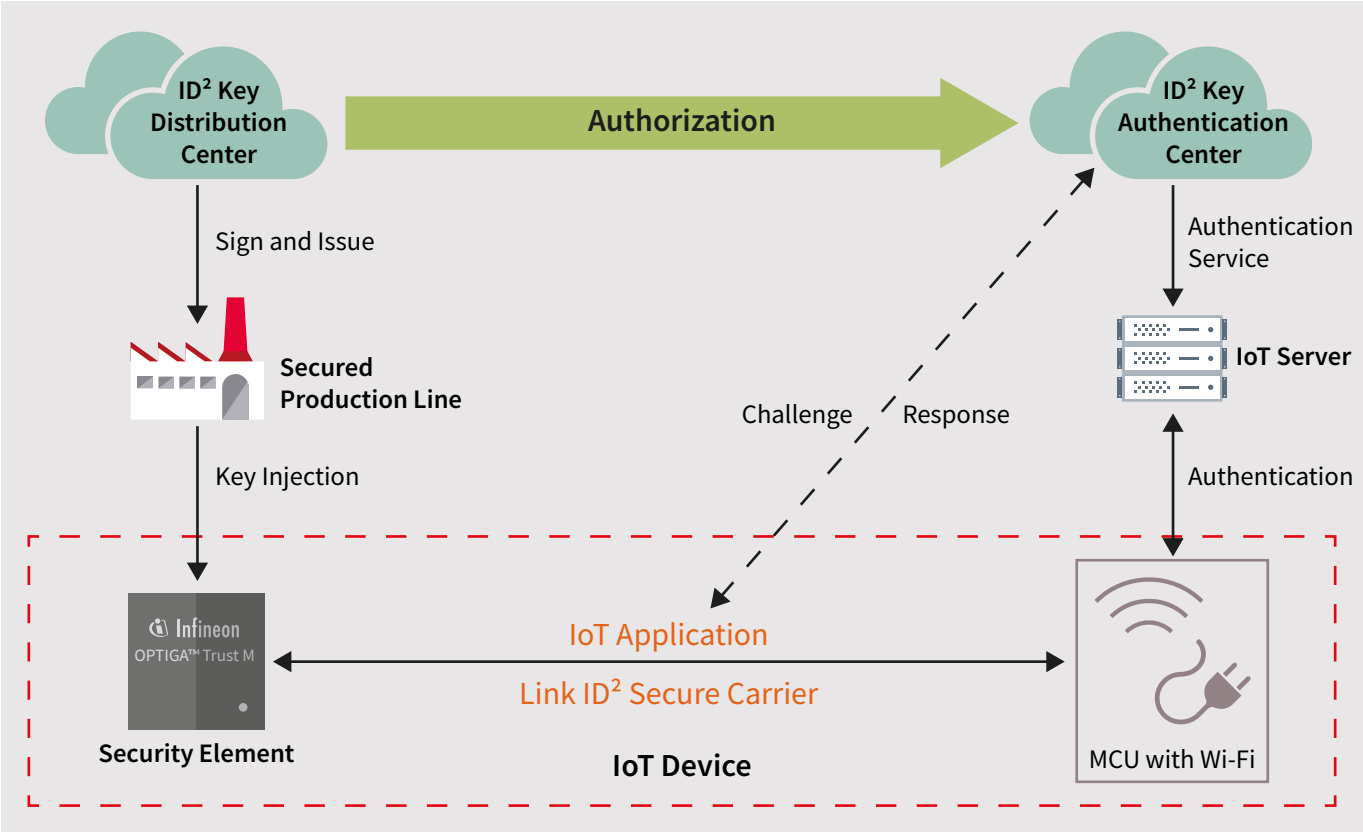


Figure 2: Ali Cloud Link ID² infrastructure

It provides the key infrastructure enabling "things" and services to securely connect. Link ID² supports multiple security level carriers to strike the right balance between security, cost, power consumption and other performance factors in the IoT. This paves the way for affordable, easy to use security solutions for customers, allowing them to adapt to the fragmented market demands of the IoT.

Ali Cloud Link ID² platform contains two services: a key distribution center and an authentication center. The distribution center uses hardware encryption machines and secured storage technology to protect key generation and storage. It connects with the partner's secured production line for secured insertion of the key into the secure carrier of various security levels.

The customer integrates the secure carrier into the IoT device, initiates the device authentication, information encryption and other interfaces provided cloud to establish a safe channel for the non-repudiation, integrity and confidentiality of business data.

3. Alibaba Cloud IoT security

Alibaba Cloud has invested considerable effort into securing the Ali Cloud Link ID² infrastructure and services. In this section we introduce the Ali Cloud Link ID² IoT security measures.

3.1 Ali Cloud Link ID² authentication process

Figure 3 depicts software IoT device authentication with the unique device ID and symmetric key. The IoT device uses the unique ID to authenticate the device with the Link ID² Authentication Center based on send/request challenge.

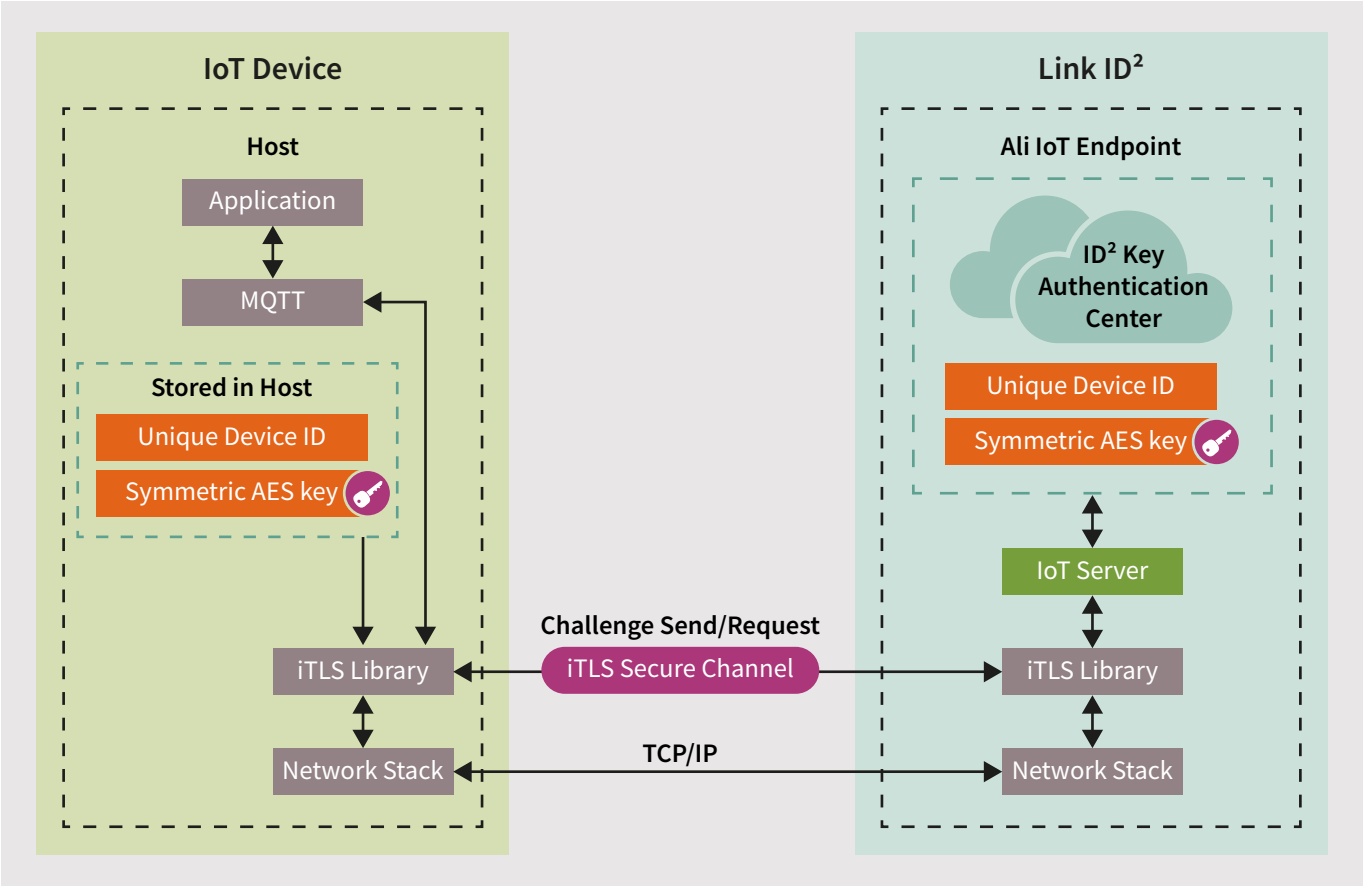


Figure 3: Software based Link ID² platform authentication using Ali Cloud Link ID²

4. Hardening security for IoT devices using Infineon OPTIGA™ Trust M2 ID2

Depending on the IoT device and its application, the main processing component is a CPU or microcontroller, subsequently referred to as host controller.
The host controller of the IoT device handles data collection and processing functionality, as well as the remote data communication, for example, with the Alibaba Cloud.

The Alibaba Cloud Shared Security Responsibility Model demands that the IoT solution provider adequately protect its IoT devices. This section explains how hardware-based security adds strong protection measures to IoT devices.

4.1 Infineon OPTIGA™ Trust M2 ID2

The Infineon OPTIGA™ Trust M2 ID2 is a turn-key hardware plus software security module that offers the right set of security functions to protect IoT devices.

The function set of the OPTIGA™ Trust M2 ID2 includes

- Operations to manage data objects such as the unique device ID
- Operations to manage key objects such as the AES/RSA key
- A toolbox with cryptographic primitives and functions (for example asymmetric encrypt and decrypt, etc.)

The toolbox is a collection of cryptographic functions that enable or enhance cryptographic protocols that are not implemented inside the Infineon OPTIGA™ Trust M2 ID2. Use cases such as platform integrity or secured communication can be implemented using the following toolbox components:

- Symmetric encryption using AES.
- Symmetric decryption using AES.

4.2 Integration with an Alibaba Cloud connected IoT device

The most important OPTIGA™ Trust M2 ID2 functions for securing the Ali Cloud Link ID² connection are those related to key and certificate management and iTLS protocol support.

Figure 4 depicts the system architecture of an IoT solution with an IoT device secured by OPTIGA™ Trust M2 ID2.
In this architecture, the OPTIGA™ Trust M2 ID2 protects the long-term cryptographic material used for the iTLS based authentication with the IoT service running on Ali Cloud Link ID² platform. The OPTIGA™ Trust M2 ID2 thereby safeguards, and securely stores:

› the long-term unique device ID,
› the long-term private key of the IoT device, which corresponds to the unique device ID

Compared with the software-based security solution outlined in Section 3, the hardware-based secured solution depicted in Figure 4 implements only a minor (device ID storage and symmetric encrypt/decrypt) portion of the iTLS library.

The shielded connection [2] establishes secured and protected communication channel over the I²C interface as depicted in Figure 4.

Electrically, the OPTIGA™ Trust M2 ID2 is connected via the I2C bus to the IoT device host controller. The Infineon I2C Protocol Stack library enables communication with the Infineon OPTIGA™ Trust M2 ID2 product. The protocol stack consists of multiple layers that relate to the ISO Open Systems Interconnection (OSI) model. A host controller specific Hardware Abstraction Layer (HAL), which interfaces to a host's I2C driver or I2C peripheral enables flexible host controller support.

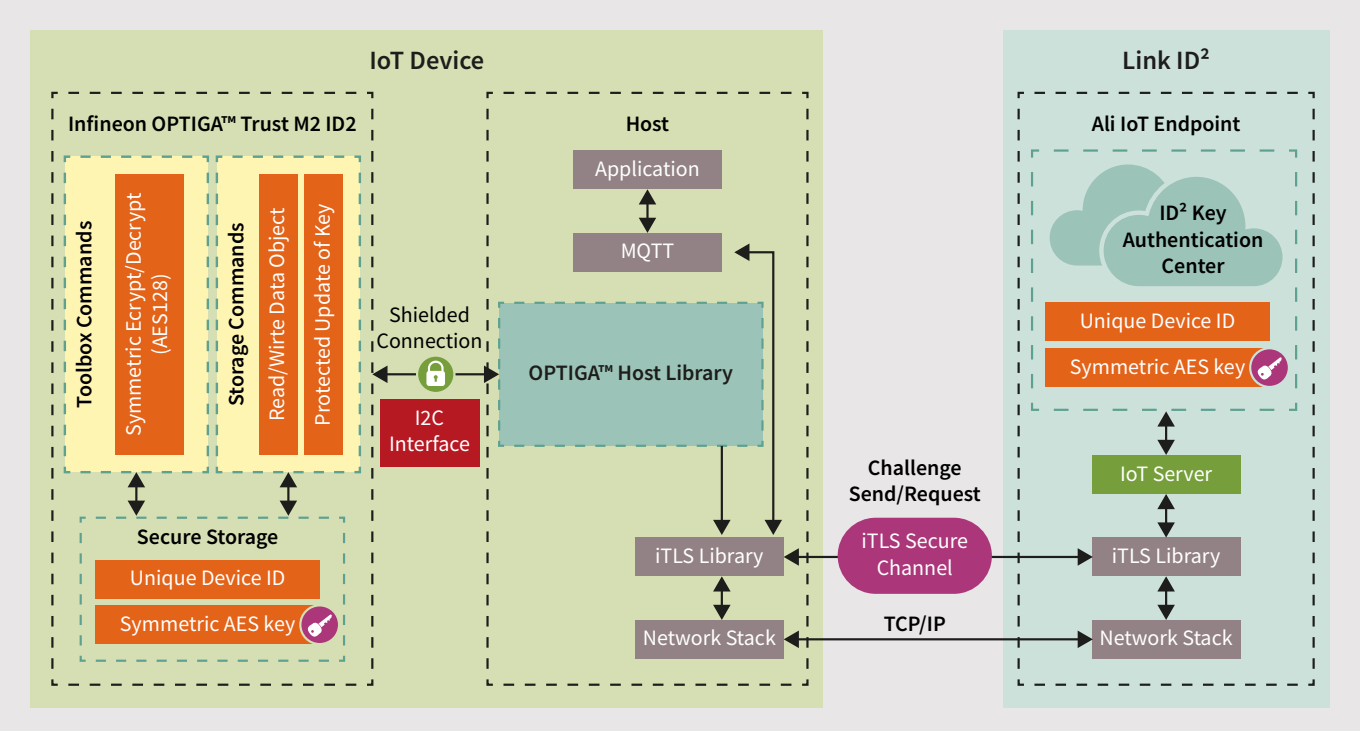


Figure 4: Overview of (Infineon OPTIGA™ Trust M2 ID2) integration with Ali Cloud Link ID²

4.3 Device enrollment process at Alibaba Cloud IoT

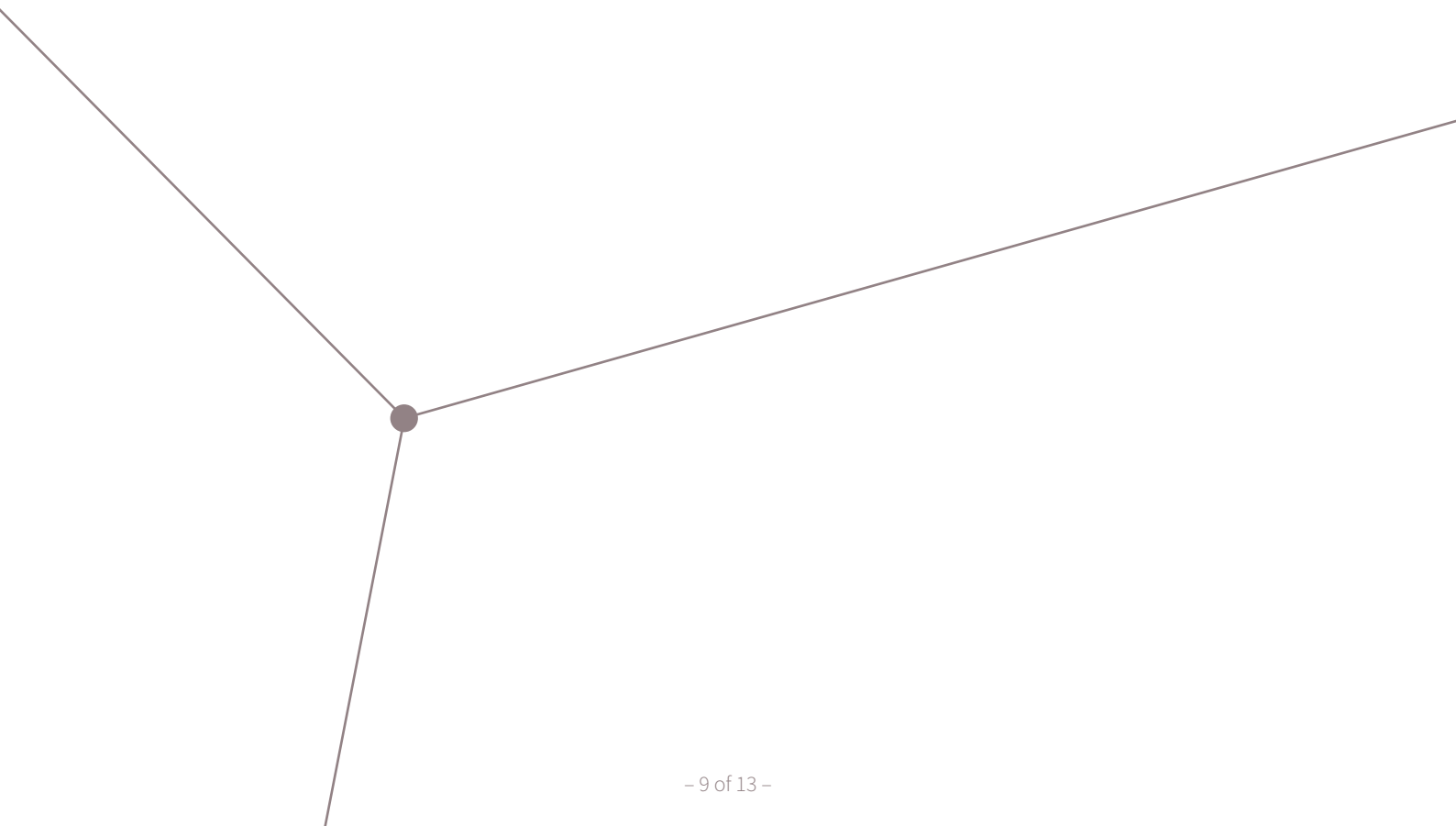
Creating a device is a customized process based on the customer's security needs. To customize device enrolment, contact Alibaba Cloud Services.

4.4 Hardware-based security

The Infineon OPTIGA™ Trust M2 ID2 offers a wide range of cryptographic services that protect other important security features that are needed for IoT devices:

- Secured device firmware update and secured software update
- Secured boot, measured boot, and platform integrity
- Protected update of data (for example, Device ID) installed on OPTIGA™ Trust M2 ID2
- Counters either for generic usage or to limit the usage of secrets installed on OPTIGA™ Trust M2 ID2
- Hibernate/restore option to reduce power consumption which is important for battery based, low power devices.

Please visit https://github.com/Infineon/OPTIGA-Trust-M2-ID2 to download the open source (MIT license) host libraries to integrate OPTIGA™ Trust M2 ID2.



5. Conclusion

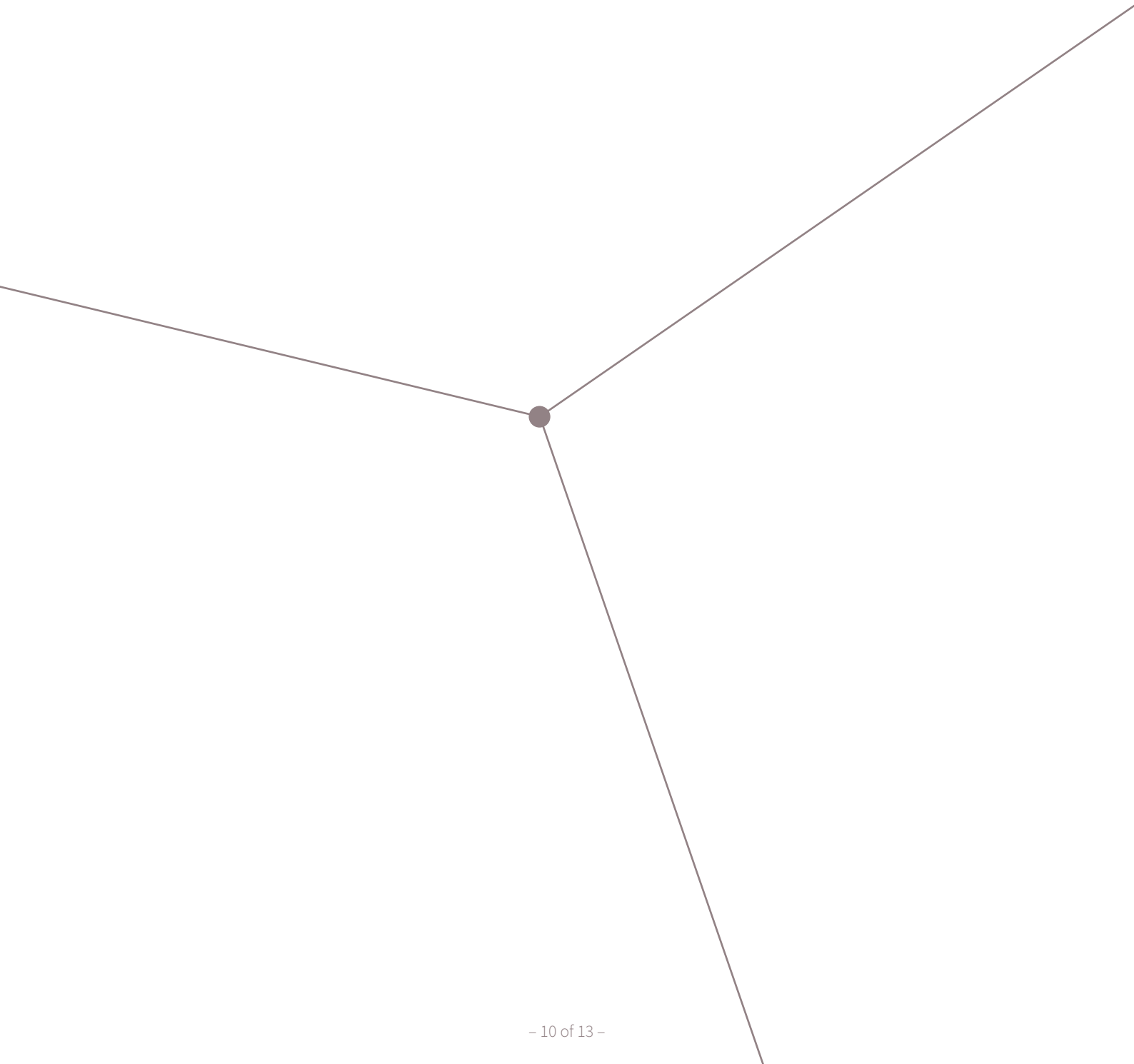
Cloud services are an essential enabler of the IoT.
Both protected communication and device authentication are of utmost importance, and they must be implemented from the very beginning of the device design process and cover, the complete product life cycle.

This paper provides an overview of Ali Cloud Link ID^2 infrastructure and device authentication process using a unique device ID and corresponding key.

Technically, OPTIGA™ Trust M2 ID2 hardens device security and supports the security integration process by offering:

- Flexibility – OPTIGA™ Trust M2 ID2 can be integrated with different host platforms and TLS libraries – from proprietary customer options to proven open source solutions
- Ease of use – host side library which includes Infineon I2C protocol, APIs for toolbox and read/write functionalities.

In conclusion, Infineon's OPTIGA™ Trust M2 ID2 enables the implementation of secured IoT devices based on tamper resistant hardware combined with a tailored set of ready to use security functions.



6. Glossary

Alibaba Cloud Services	Collection of public cloud services offered by Alibaba Cloud
Application Programming Interface	Set of protocols and programmatic methods/functions to programmatically interface with software or a library
ID^2	Internet Device ID
Message Queuing Telemetry Transport (MQTT)	Publish/subscribe based messaging protocol
Software development kit (SDK)	Set of software development tools to create an application
Toolbox	In the context of the Infineon OPTIGA™ Trust M2 ID2, toolbox refers to a set of cryptographic functions that can be used to implement TLS
Transport Layer Security (TLS)	Cryptographic protocol for secured Internet communication that runs on top of TCP
Transmission Control Protocol (TCP)	Transport layer Internet protocol that provides reliable, ordered, and error checked delivery of a stream of octets between applications running on hosts communicating via an IP network

7. References

[1] About Alibaba Cloud.
https://www.alibabacloud.com/about?spm=a3c0i.7911826.1389108.dnavwhya2.4f9a14b3InbkbZ

[2] Shielded connection
https://github.com/Infineon/optiga-trust-m/wiki/Shielded-Connection-101

Where to buy

Infineon distribution partners and sales offices:
www.infineon.com/WhereToBuy

Service hotline

Infineon offers its toll-free 0800/4001 service hotline as one central number, available 24/7 in English, Mandarin and German.

- Germany ..... 0800 951 951 951 (German/English)
- China, mainland ..... 4001 200 951 (Mandarin/English)
- India ..... 000 800 4402 951 (English)
- USA ..... 1-866 951 9519 (English/German)
- Other countries ..... 00* 800 951 951 951 (English/German)
- Direct access ..... +49 89 234-0 (interconnection fee, German/English)

* Please note: Some countries may require you to dial a code other than "00" to access this international number. Please visit www.infineon.com/service for your country!

Mobile product catalog

Mobile app for iOS and Android.

www.infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 03/2021

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.