Kigen
An Arm Company

orange™

Growing a secure ecosystem for IoT Devices

AGENDA

iSIM Momentum

IoT SAFE Overview

IoT SAFE in Action

Kigen

An Arm Company

orange™

Welcome to Kigen, An Arm Company

Kigen
An Arm Company

Mission
Secure Connected Devices

Vision
Drive eSIM to be the cornerstone of IoT Security

Scalability & Trust are the two principles supporting our vision

Hello

orange™

A Multi-service Operator

- Present in 26 countries
- 8th Telco brand in the world
- Orange Live Objects platform connects 16 million IoT devices

Our Engagements

- Accelerate the transformation of IT services for B2B customers in IoT and smart mobility
- Scale up cybersecurity and instill more trust in IoT devices
- Put Data and AI at the heart of our innovation model
- Maintain our leadership in connectivity with a focus on network virtualization, fiber and 5G

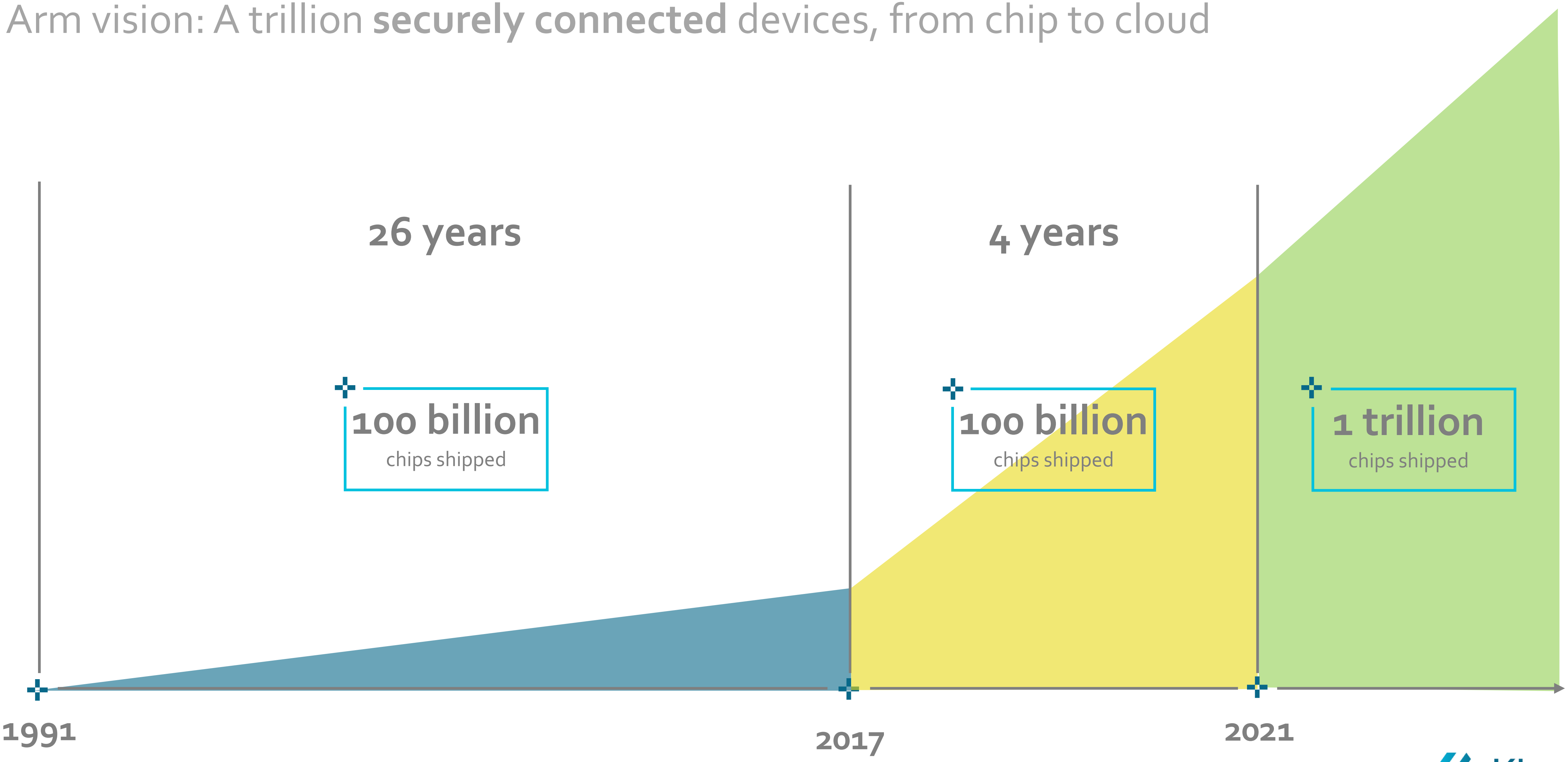
iSIM MOMENTUM

PAUL BRADLEY – DIRECTOR OF STRATEGY & INNOVATION, KIGEN

Kigen

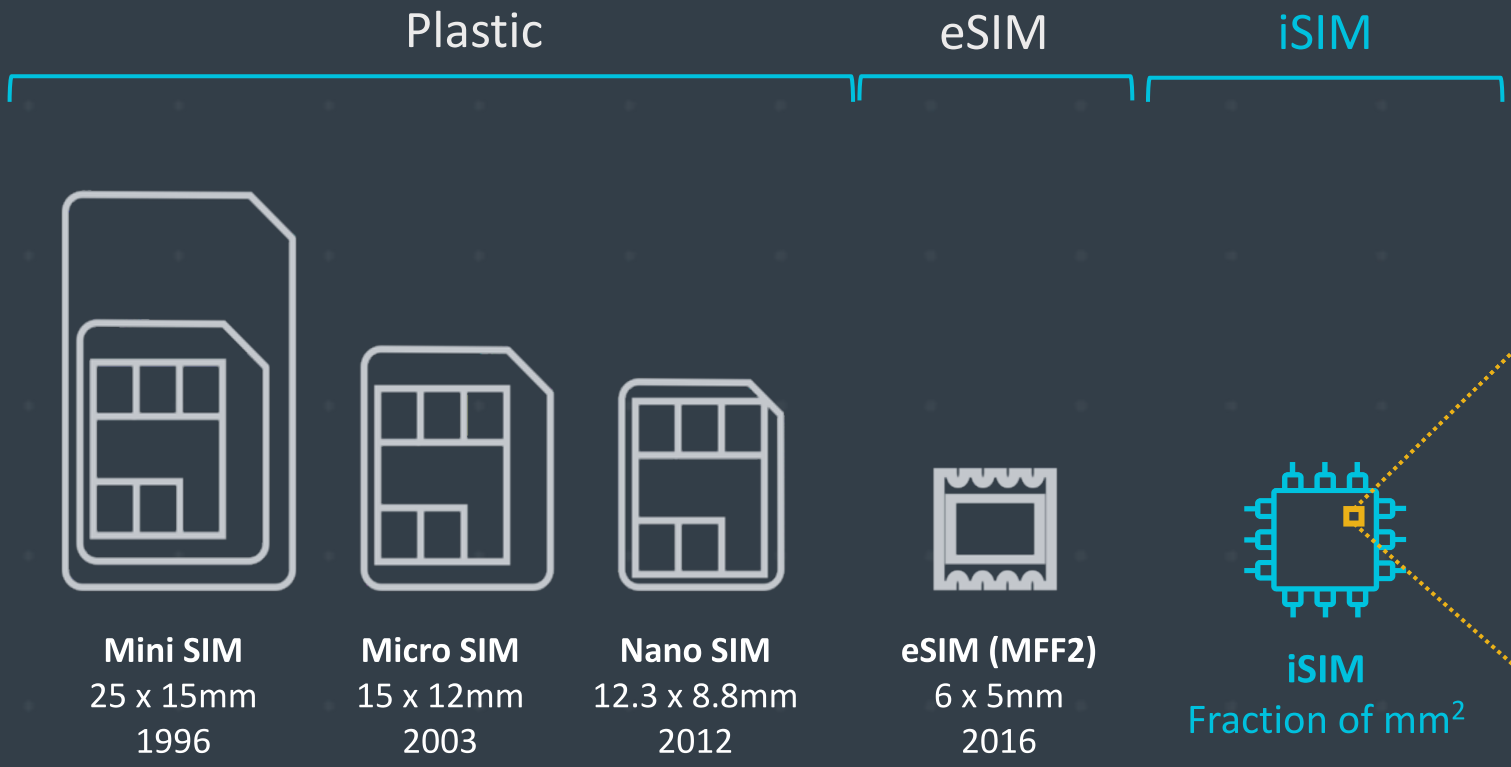
The road ahead is exciting, scalability & trust are key factors

Arm vision: A trillion **securely connected** devices, from chip to cloud



Kigen

iSIM brings SIM into the 21st century



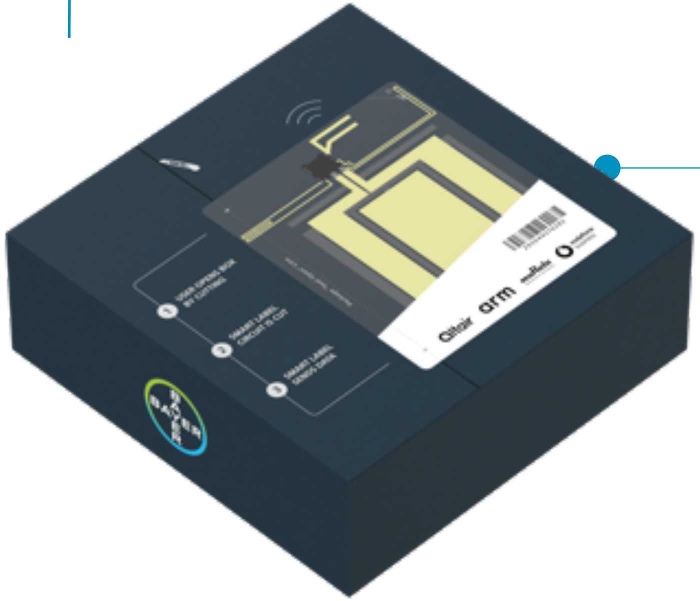
- 50% less expensive than eSIM
- Easier integration
- Power improvement (> -70%)
- 98% smaller than eSIM
- x10 performance enhancement
- Simplified logistics for ODMs
- eSIM Remote management
- New devices and business models

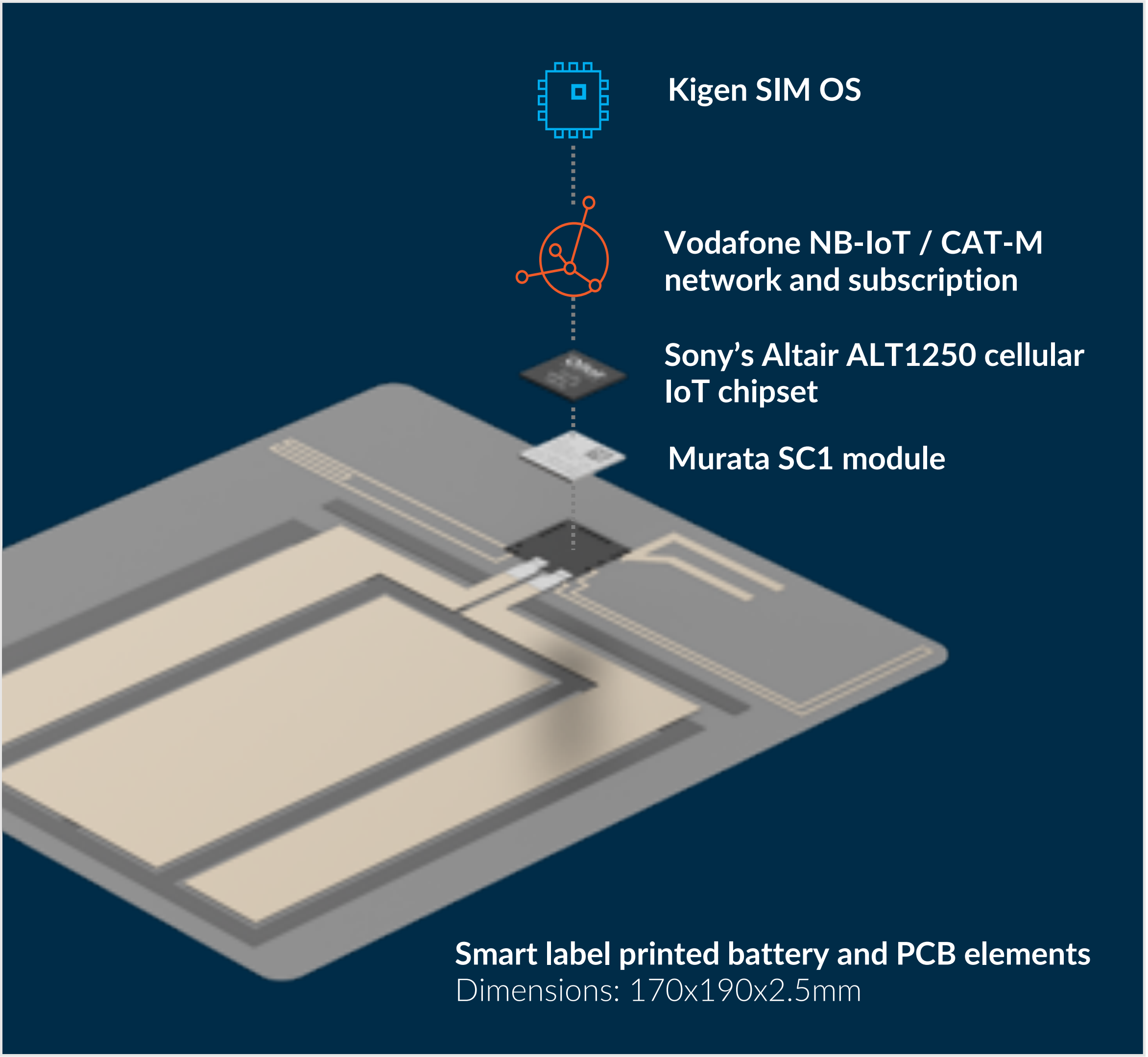
Kigen

iSIM unleashes IoT devices and services innovation

Critical data insights enabled by a two years battery life

- User opens box by cutting
- Smart label circuit is cut
- Smart label sends data





Kigen SIM OS

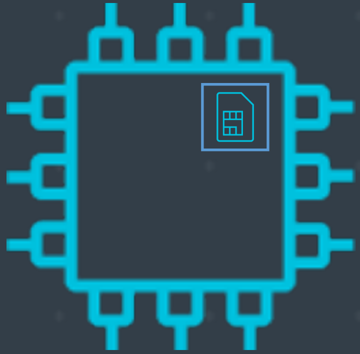
Vodafone NB-IoT / CAT-M network and subscription

Sony's Altair ALT1250 cellular IoT chipset

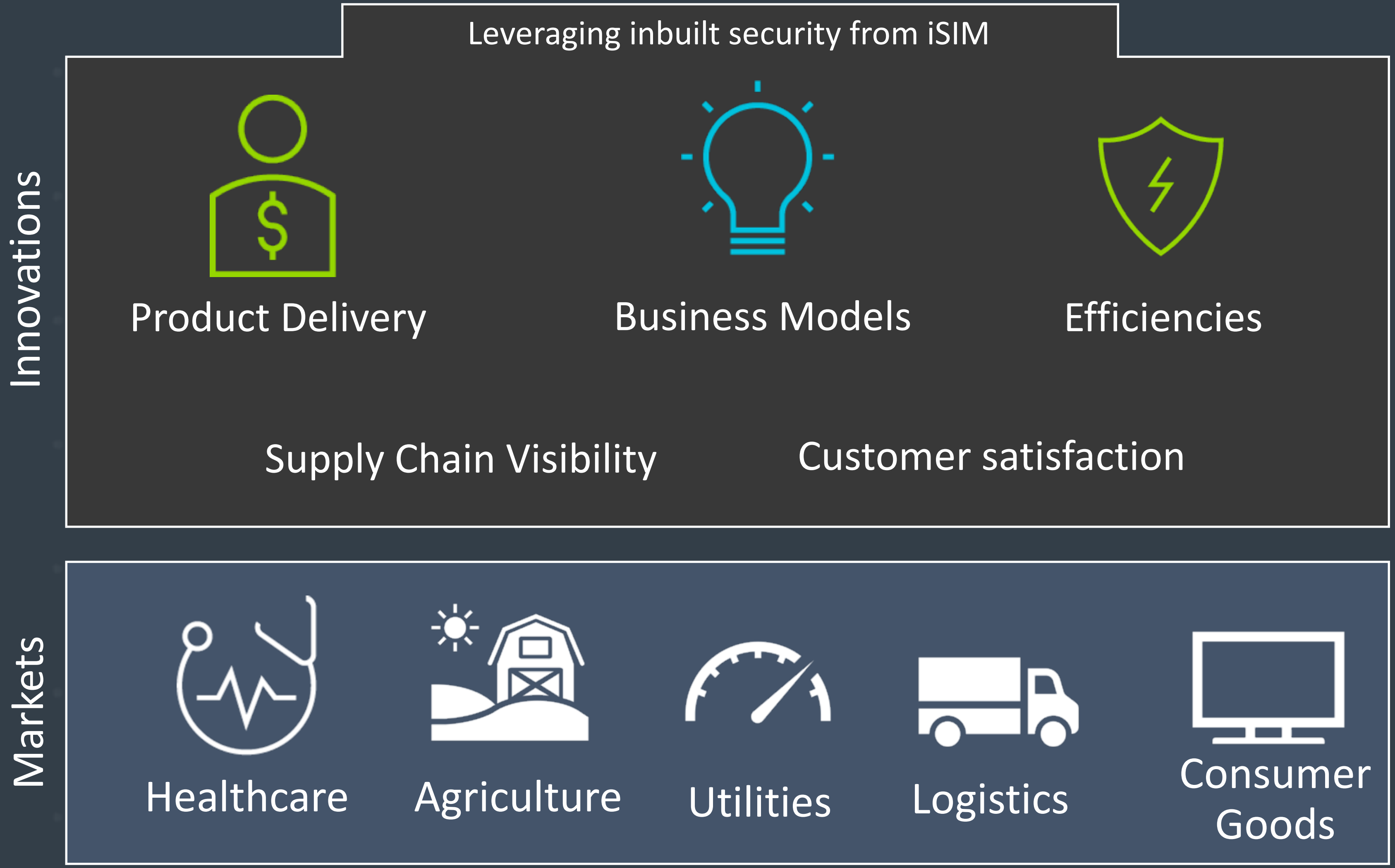
Murata SC1 module

Smart label printed battery and PCB elements
Dimensions: 170x190x2.5mm

Additional iSIM use cases



Leveraging iSIM
and IoT technologies to
develop new business
models



Leveraging inbuilt security from iSIM

Innovations

Product Delivery

Business Models

Efficiencies

Supply Chain Visibility

Customer satisfaction

Markets

Healthcare

Agriculture

Utilities

Logistics

Consumer Goods

IoT SAFE

LEILA DE CHARETTE – IoT STANDARDISATION ENGINEER, ORANGE

PAUL BRADLEY – DIRECTOR OF STRATEGY & INNOVATION, KIGEN

ANURAG SHARMA – SENIOR SOFTWARE DEVELOPER & IoT SAFE R&D LEAD, KIGEN

IoT SAFE:
A Result of Industry Wide Collaboration

TCA TRUSTED CONNECTIVITY ALLIANCE
ST life.augmented
TELUS
verizon
vodafone
Telefonica
infineon
achelos
G+D
VALID
ERICSSON
Telstra
ublox
bics
AT&T
UL
中国移动 China Mobile
TIM
IDEMIA
orange
JT
Kigen An Arm Company
THALES
Microsoft

Mobile Network Operators

Cloud Providers

Device Makers

Modem Makers

SIM Providers

Network Infrastructure Providers

Secure IC Vendors

Enabling Strong Security in IoT

IoT SAFE

Leveraging a hardware secure element as a root of trust to protect sensitive assets (keys)

SECURE implies protecting data using the credentials inside the hardware secure element.

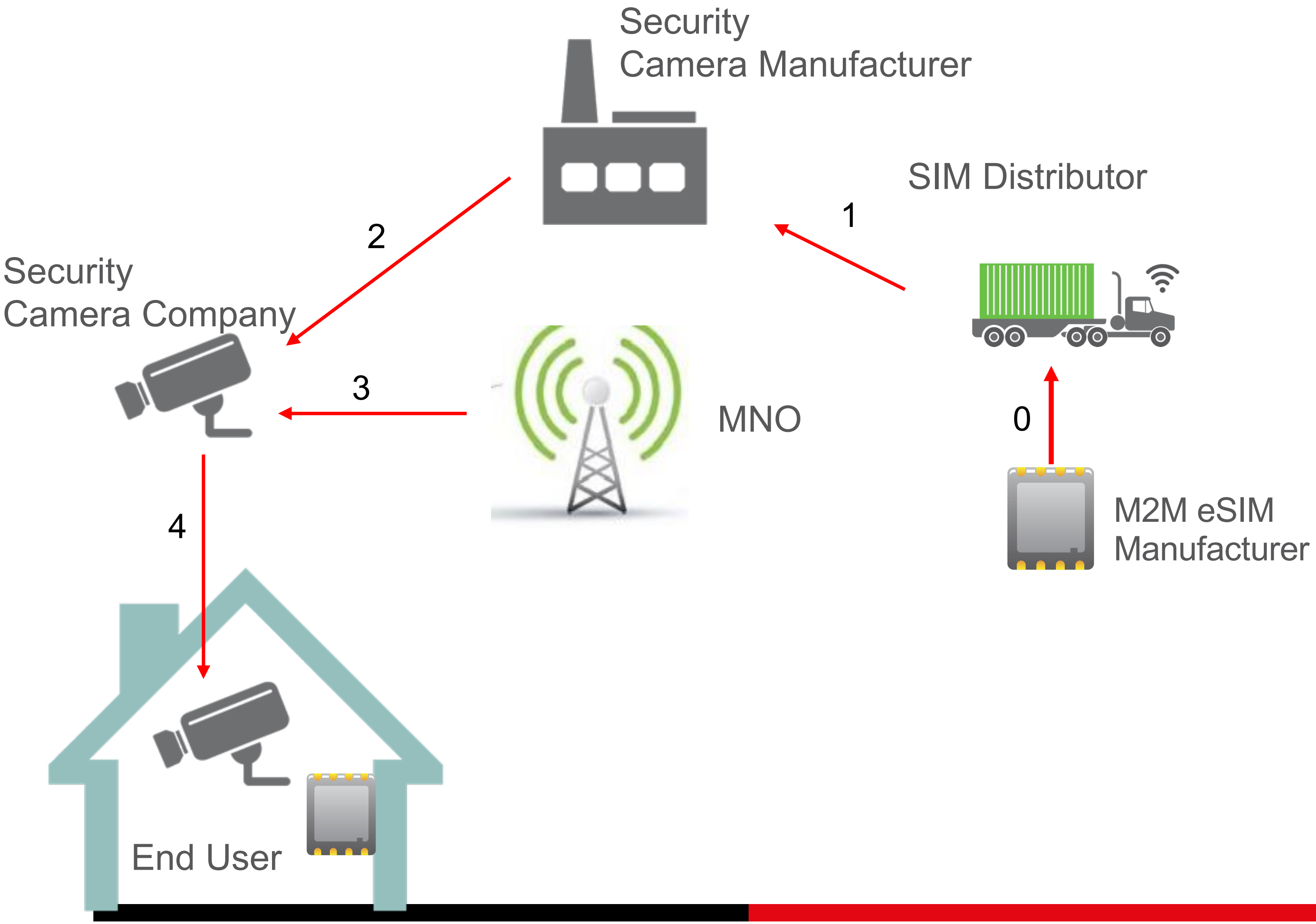
An iSIM has advanced security and cryptographic features and enables interoperability

Use the iSIM as a robust, scalable and standardised solution to protect IoT data from chip to multi-cloud.

Benefits of IoT SAFE

1. High security protection for end-to-end credentials
2. Optimise certificate renewal cycles (constrained)
3. Unified Zero Touch Provisioning
4. Value-Add & Trust for IoT Service Providers

Use Case: Deployment of eSIM in Security Camera(1/2)



0. eSIMs are sold in open market by the M2M-eSIM manufacturer

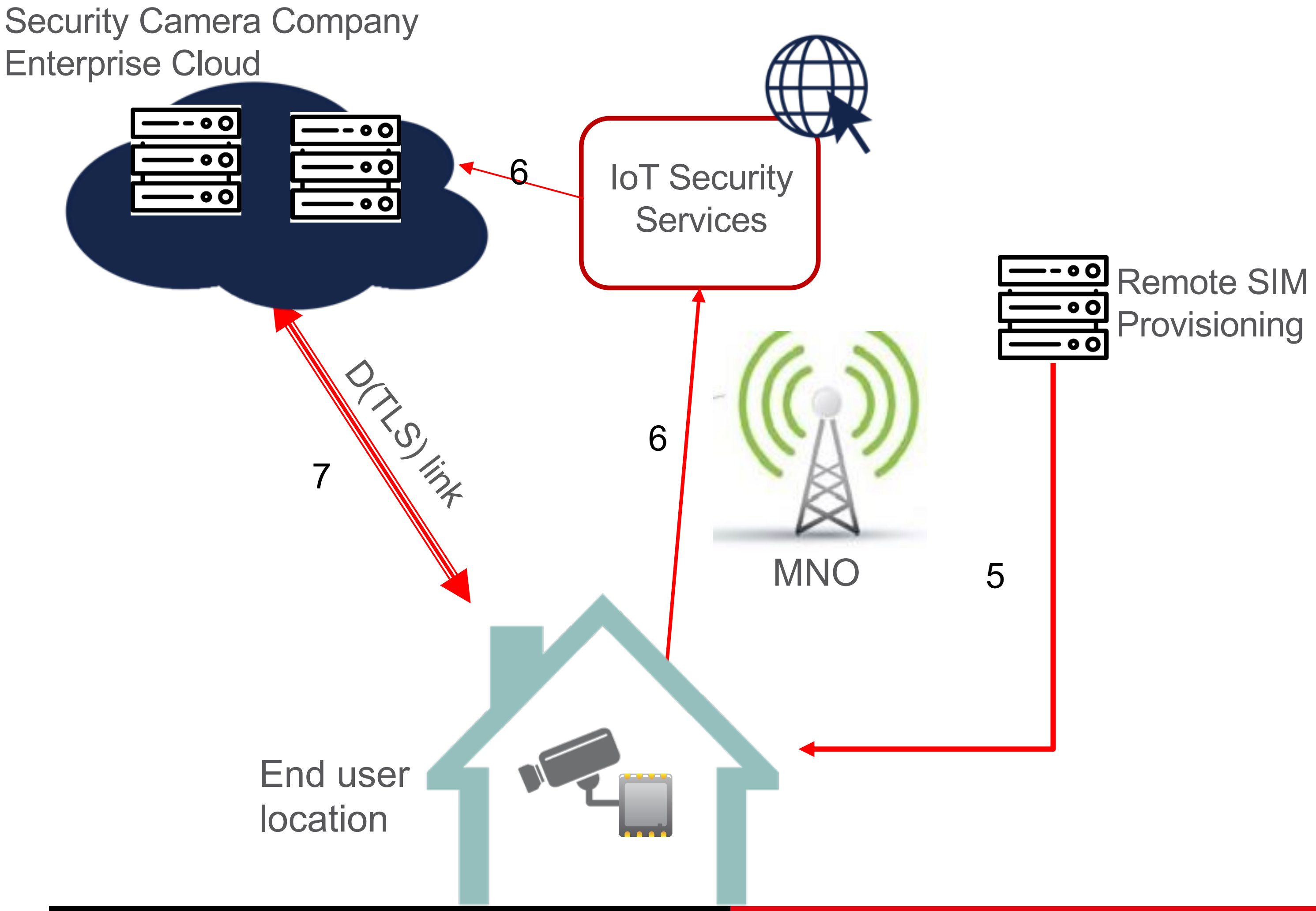
1. Security Camera Manufacturer buys M2M-eSIM from a distributor

2. Security Camera Company buys security cameras from Security Camera Manufacturer

3. Security Camera Company buys connectivity from MNO

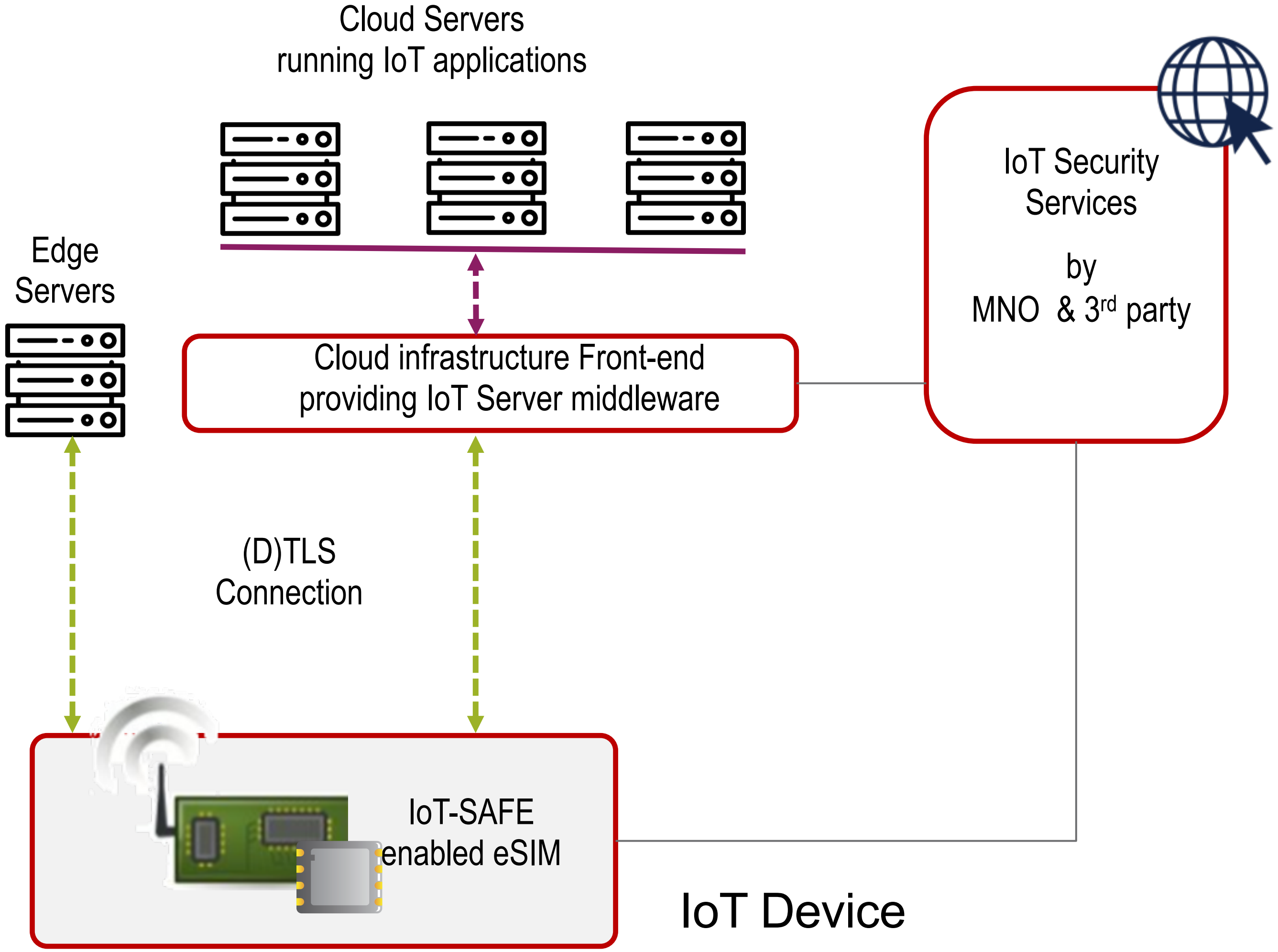
4. End user buys security services from Security Camera Company

Use Case: Deployment of eSIM in Security Camera(2/2)



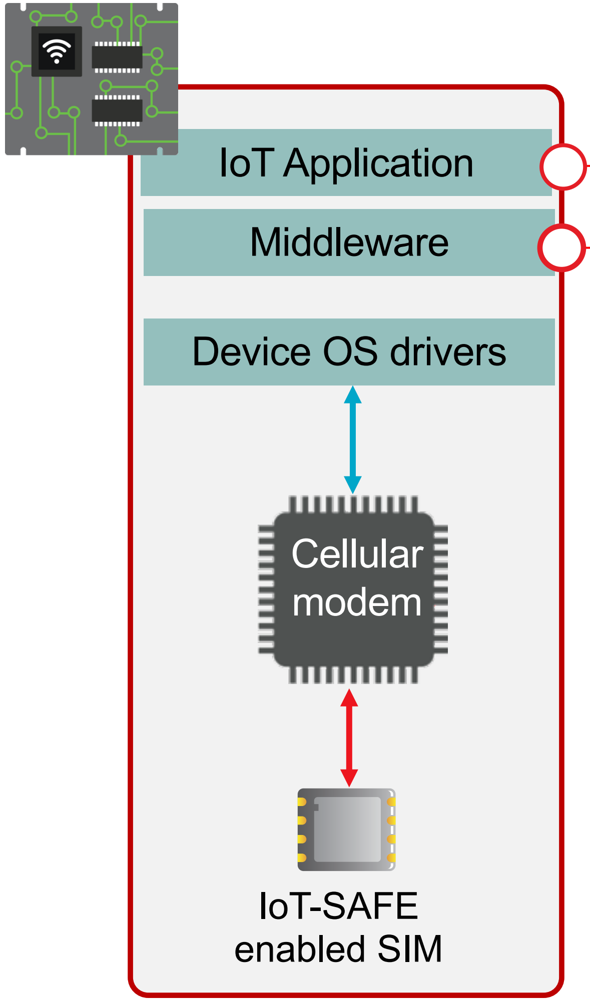
5. First time the camera is installed, SIM gets provisioned via Remote SIM Provisioning services
6. eSIM downloads its IoT-SAFE client certificate using IoT Security services
7. **The camera can securely connect to the cloud application using a standard (D)TLS handshake**

IoT-SAFE System Reference Architecture


Cloud Servers running IoT applications
Edge Servers
Cloud infrastructure Front-end providing IoT Server middleware
IoT Security Services by MNO & 3rd party
(D)TLS Connection
IoT-SAFE enabled eSIM
IoT Device

- IoT devices can securely perform mutual (D)TLS authentication to an IoT server:
  - Client-side certificate stored in IoT-SAFE
  - Supports asymmetric or symmetric schemes
  - Server certificate check done by IoT-SAFE
- IoT-SAFE keeps long-term keys secret.
- Enables provisioning and credential lifecycle management from a Remote IoT security service
- IoT-SAFE Certificate & Secrets can be managed by a IoT Security Service entity

Enablement



Having the Device Middleware enabled for IoT-SAFE is key for a successful market deployment

- IoT application to be IoT-SAFE agnostic
- Facilitate higher security among non-SIM experts by abstracting SIM complexity in TLS stack

IoT-SAFE Middleware key features

- Transparent to Application developer, as much as possible. Developer calls usual APIs in TLS stack
- Middleware to hide SIM-handling complexity
- Applet should still be accessible for specific functions

Examples of TLS stacks within device middleware:

- openSSL for embedded Linux platforms (link)
- Mbed tls for Mbed platforms (link)
- Wolf ssl for various embedded platform (link)
- Bearssl for constrained devices (link)

IoT SAFE in Action

FABRICE FONTAINE – EMBEDDED SYSTEM SECURITY EXPERT, ORANGE

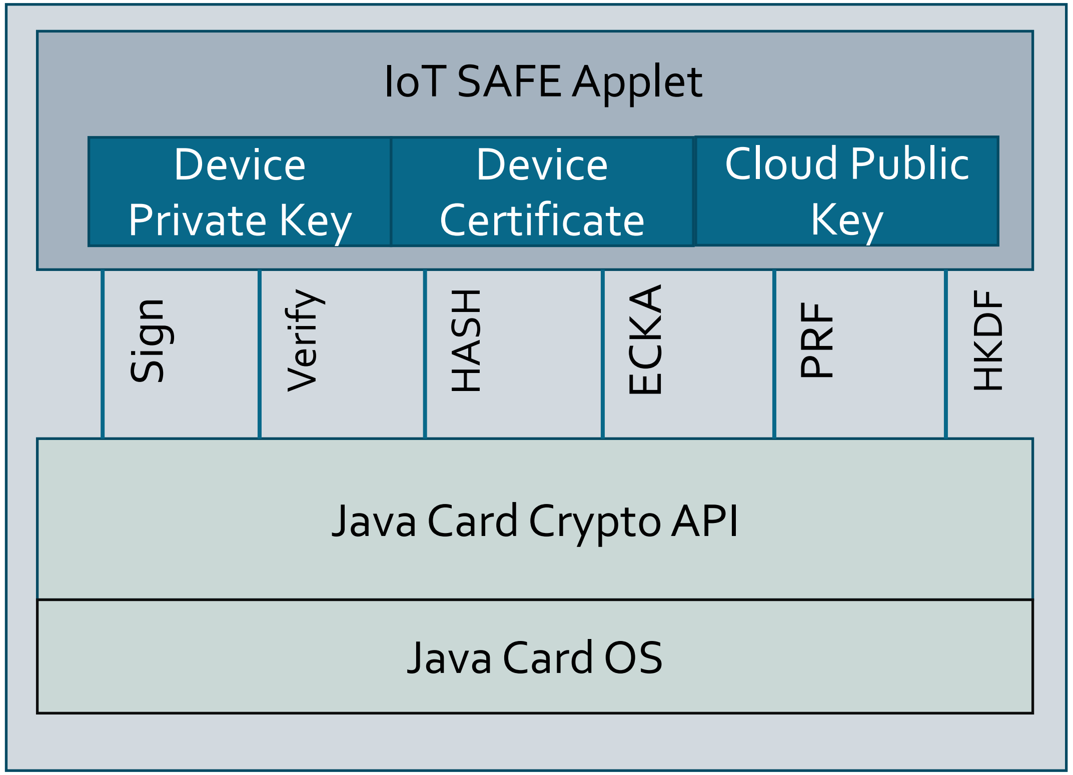
ANURAG SHARMA – SENIOR SOFTWARE DEVELOPER & IoT SAFE R&D LEAD, KIGEN

Kigen

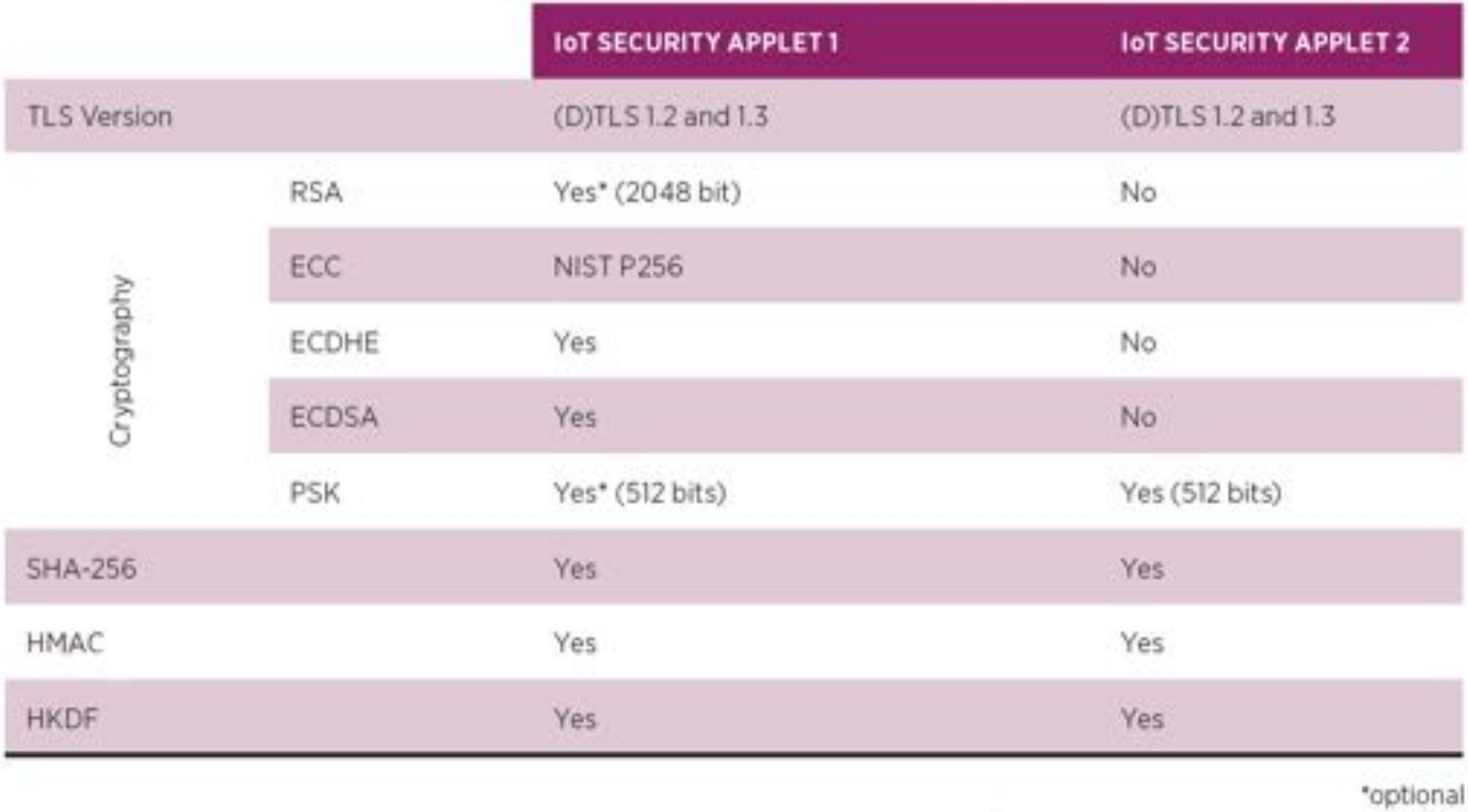
IoT SAFE applet

Overview

- Keys and Certificates are stored in objects which are identified by an ID and label.
- Object creation, editing and deletion are proprietary.
- Keys and Certificates can be updated remotely.
- Credentials can be pre-installed or set in the field.
- Can be installed in ISD-P, MNO-SD or future SAM SD
- Most importantly Java Card makes it interoperable. JC 3.0.5 is required.



Two versions of the applet are specified by GSMA



		IoT SECURITY APPLET 1	IoT SECURITY APPLET 2
TLS Version		(D)TLS 1.2 and 1.3	(D)TLS 1.2 and 1.3
Cryptography	RSA	Yes* (2048 bit)	No
	ECC	NIST P256	No
	ECDHE	Yes	No
	ECDSA	Yes	No
	PSK	Yes* (512 bits)	Yes (512 bits)
SHA-256		Yes	Yes
HMAC		Yes	Yes
HKDF		Yes	Yes

*optional

IoT SAFE applet – lessons learned

From work with Orange

Hardware requirements

Chip supporting a SC300 processor recommended to ensure a reasonable level of crypto performance

Secure Key Provisioning at Perso

Mechanism was added to provision keys at the secure perso stage in case the cloud is pre-determined

Application ID (AID)

Was initially not listed in the GSMA specification and was added

Developed in-house test suite

Validated IoT SAFE applet without using fixed keys, every test case uses randomly generated keys

Test Specs

Trusted Connectivity Alliance work is ongoing, meaning further interoperability assurances will be available as soon as those specs are available (ETA Q1 2021) and implemented

Next Generation IoT Starter Kits: an IoT SAFE prototype

Orange IoT Cloud platform: Live Objects

orange

Datavenue

Live Objects

Live Objects

Live Objects to simplify IoT infrastructure for companies and IT integrators

Orange provides you with everything you need to plug in and keep your IoT devices running. Your data is available in the cloud of your choice in a end-to-end secure way.

Multi-connectivity

- IoT networks (2/3/4G, LoRa®*, LTE-M, NB-IoT)
- Protocols (MQTT,websockets, Rest, LoRa®*, SMS)
- IoT Edge computing for industrial use cases**
- CoAP protocol on demand (beta)
- LoRa® gateways to extend coverage*
- Gateways and device cloud connection**
- Securing messages by API keys or SSL certificates
- Connect to private Kerlink LoRa gateways**

Orange Live Objects IoT Starter Kits: IoT SAFE target

Very constrained devices (Arduino)

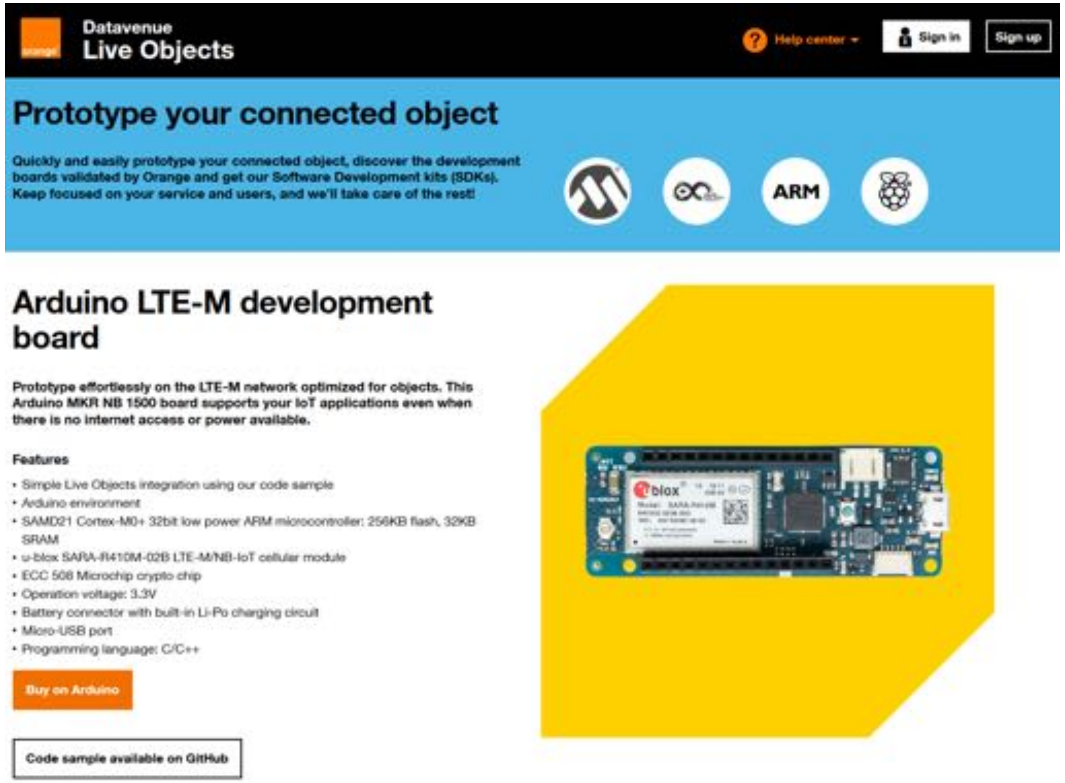
- TLS client embedded in (e)SIM
- Hard and costly to update
- No “strong” client authentication

Less constrained devices (Raspberry Pi)

- TLS client in rich OS
- Certificates and private keys are easily accessible for an attacker

IoT SAFE is a hybrid solution: TLS client in rich OS with keys in (e)SIM

So we prototyped it on the most recent, constrained device: the Arduino MKR NB 1500 with its 32 KB of RAM



Prototype your connected object

Quickly and easily prototype your connected object, discover the development boards validated by Orange and get our Software Development kits (SDKs). Keep focused on your service and users, and we'll take care of the rest!

Arduino LTE-M development board

Prototype effortlessly on the LTE-M network optimized for objects. This Arduino MKR NB 1500 board supports your IoT applications even when there is no internet access or power available.

Features

- Simple Live Objects integration using our code sample
- Arduino environment
- SAMD21 Cortex-M0+ 32bit low power ARM microcontroller: 256KB flash, 32KB SRAM
- u-blox SARA-R410M-02B LTE-M/NB-IoT cellular module
- ECC 508 Microchip crypto chip
- Operation voltage: 3.3V
- Battery connector with built-in Li-Po charging circuit
- Micro-USB port
- Programming language: C/C++

Buy on Arduino

Code sample available on GitHub

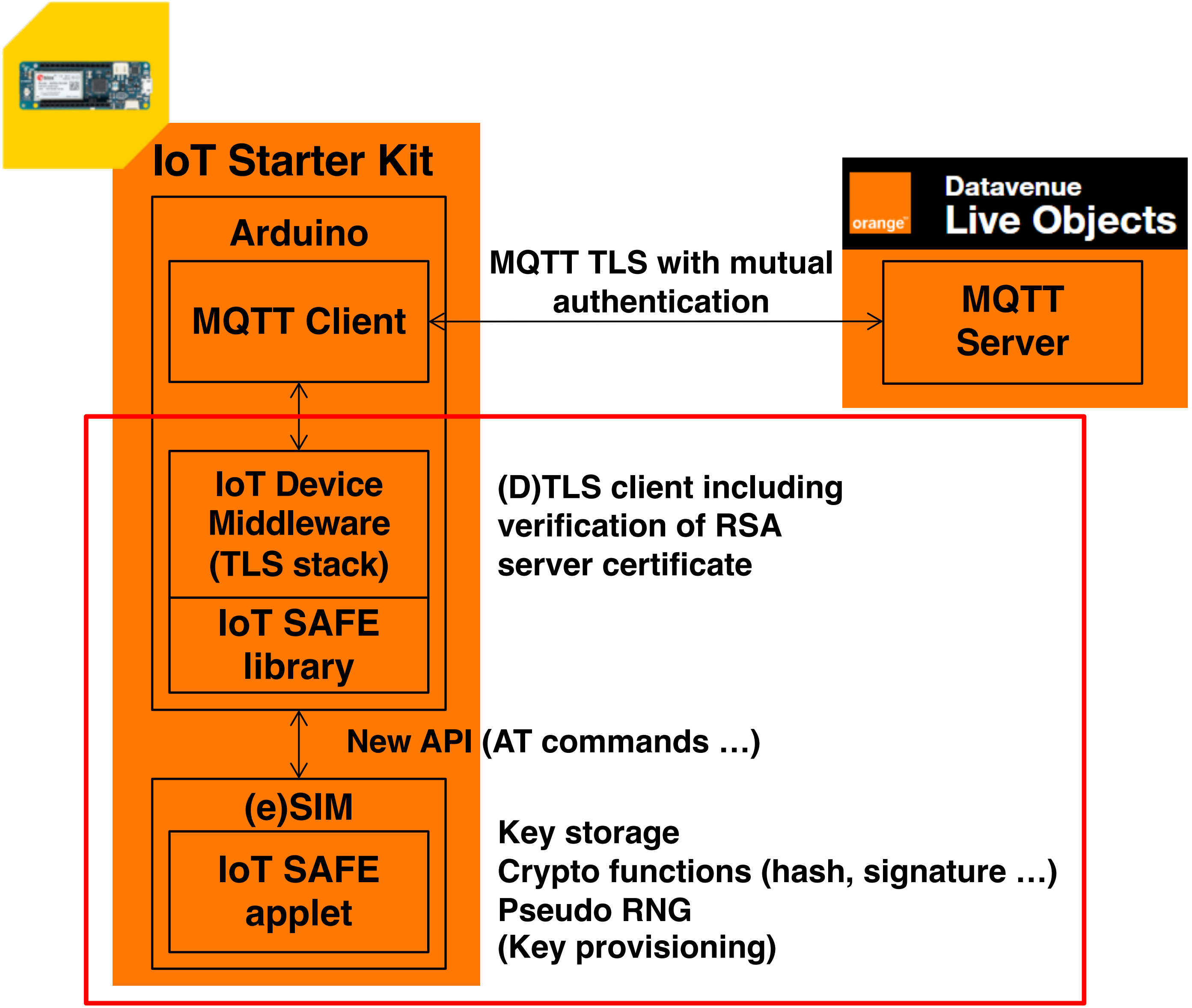
Next Gen IoT Starter Kits: prototype pre-loaded key scenario

Why?

- Check feasibility/interoperability within Orange IoT ecosystem
- Support GSMA initiative and improve the specification
- Provide a public demonstration with selected partners

Technically:

- Enable mutual authentication with ECC client certificate on Live Objects starter kit
- Pre-install IoT SAFE applet
- Develop IoT SAFE library: glue between TLS library and new SIM API



IoT Starter Kit

Arduino

MQTT Client

IoT Device Middleware (TLS stack)

IoT SAFE library

(e)SIM

IoT SAFE applet

MQTT TLS with mutual authentication

orange

Datavenue Live Objects

MQTT Server

(D)TLS client including verification of RSA server certificate

New API (AT commands …)

Key storage
Crypto functions (hash, signature …)
Pseudo RNG
(Key provisioning)

Next Gen IoT Starter Kits: key facts

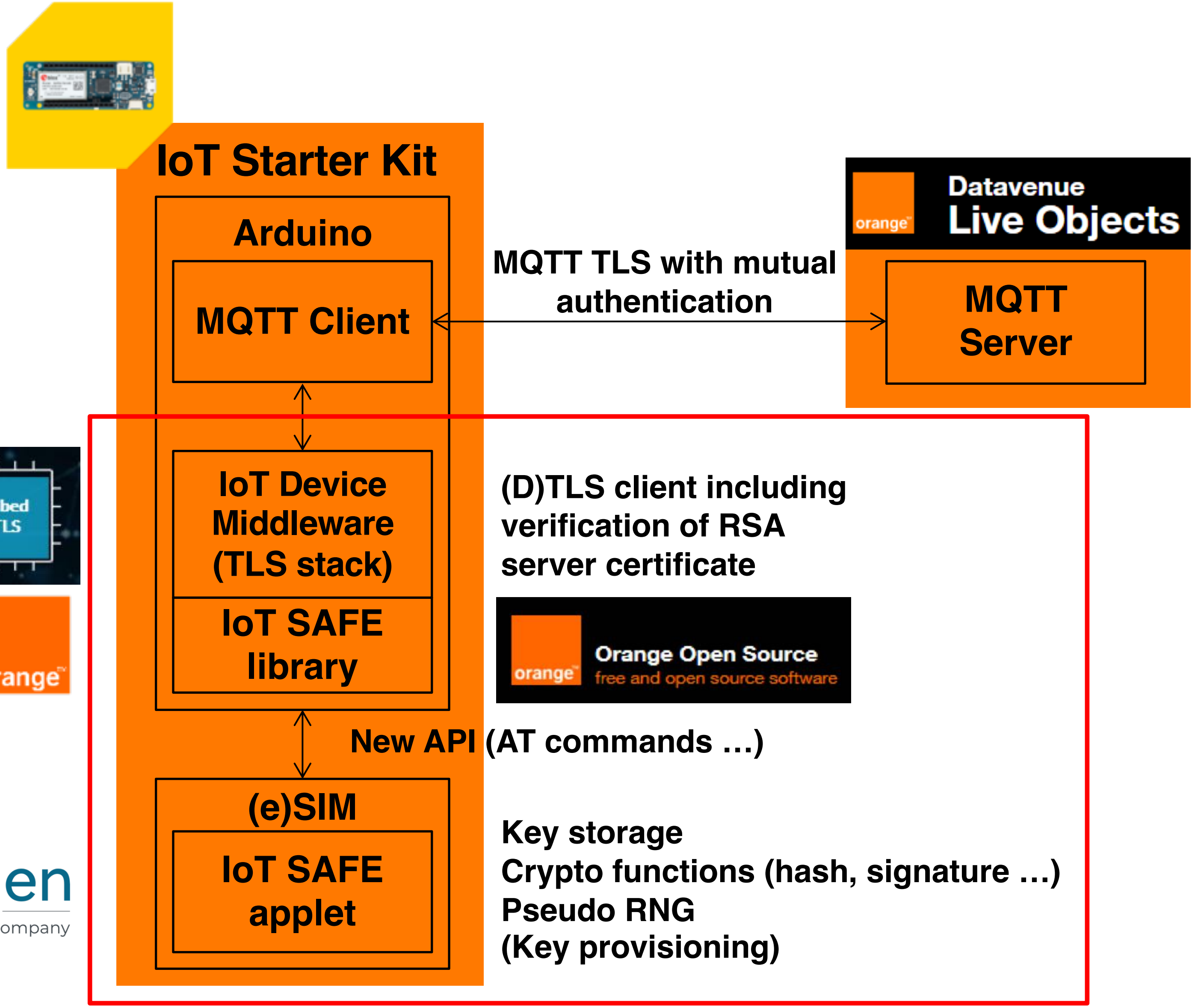
Orange IoT SAFE library:

- Tested 2 different IoT SAFE applets to verify AT/APDU interface compliance
- Tested with 2 TLS stacks: ARM mbedTLS and ArduinoBearSSL
- Open sourced since October 2020: https://github.com/Orange-OpenSource/IoT-SAFE-APDU-library

Improved specification (error code, signature format): Change Request accepted on July 2020

IoT SAFE

Kigen
An Arm Company



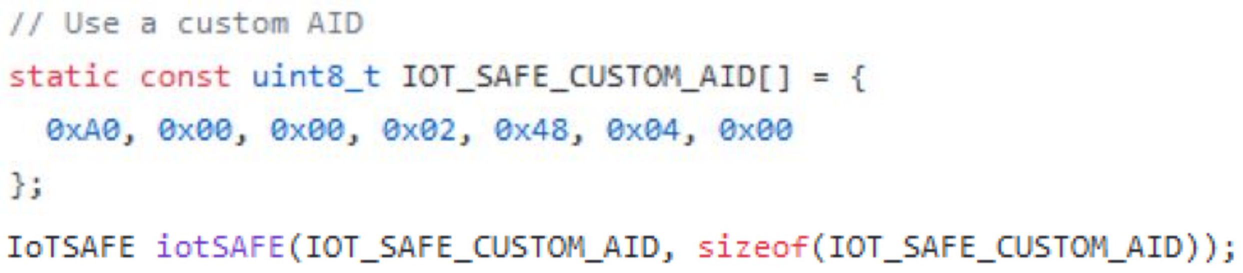
(D)TLS client including verification of RSA server certificate

Orange Open Source
free and open source software

Key storage
Crypto functions (hash, signature …)
Pseudo RNG
(Key provisioning)

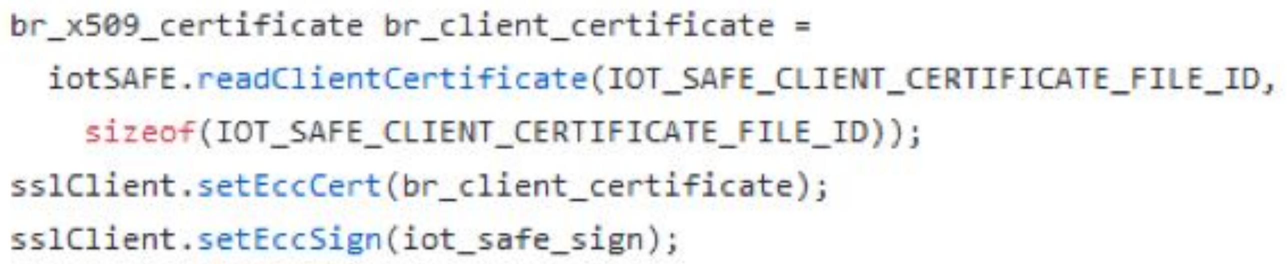
Next Gen IoT Starter Kits: extract of Arduino source code example

- Initialize IoT SAFE channel (using a custom AID, GSMA will soon standardize it)



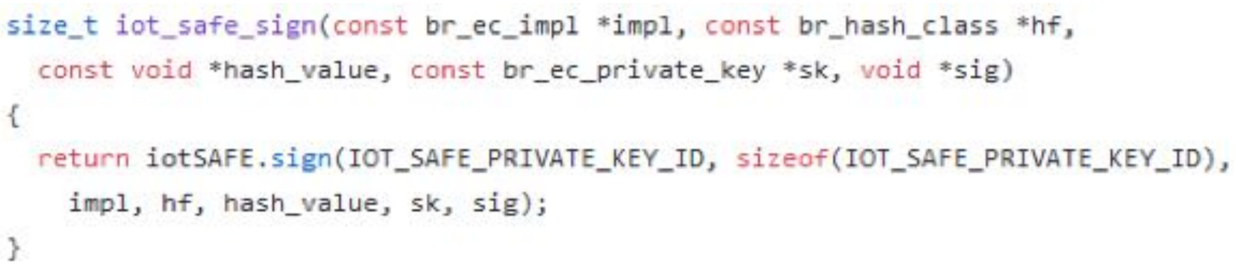
```
// Use a custom AID
static const uint8_t IOT_SAFE_CUSTOM_AID[] = {
  0xA0, 0x00, 0x00, 0x02, 0x48, 0x04, 0x00
};
IoTSAFE iotSAFE(IOT_SAFE_CUSTOM_AID, sizeof(IOT_SAFE_CUSTOM_AID));
```

- Retrieve the client certificate from the IoT SAFE applet (using a file ID or a label)



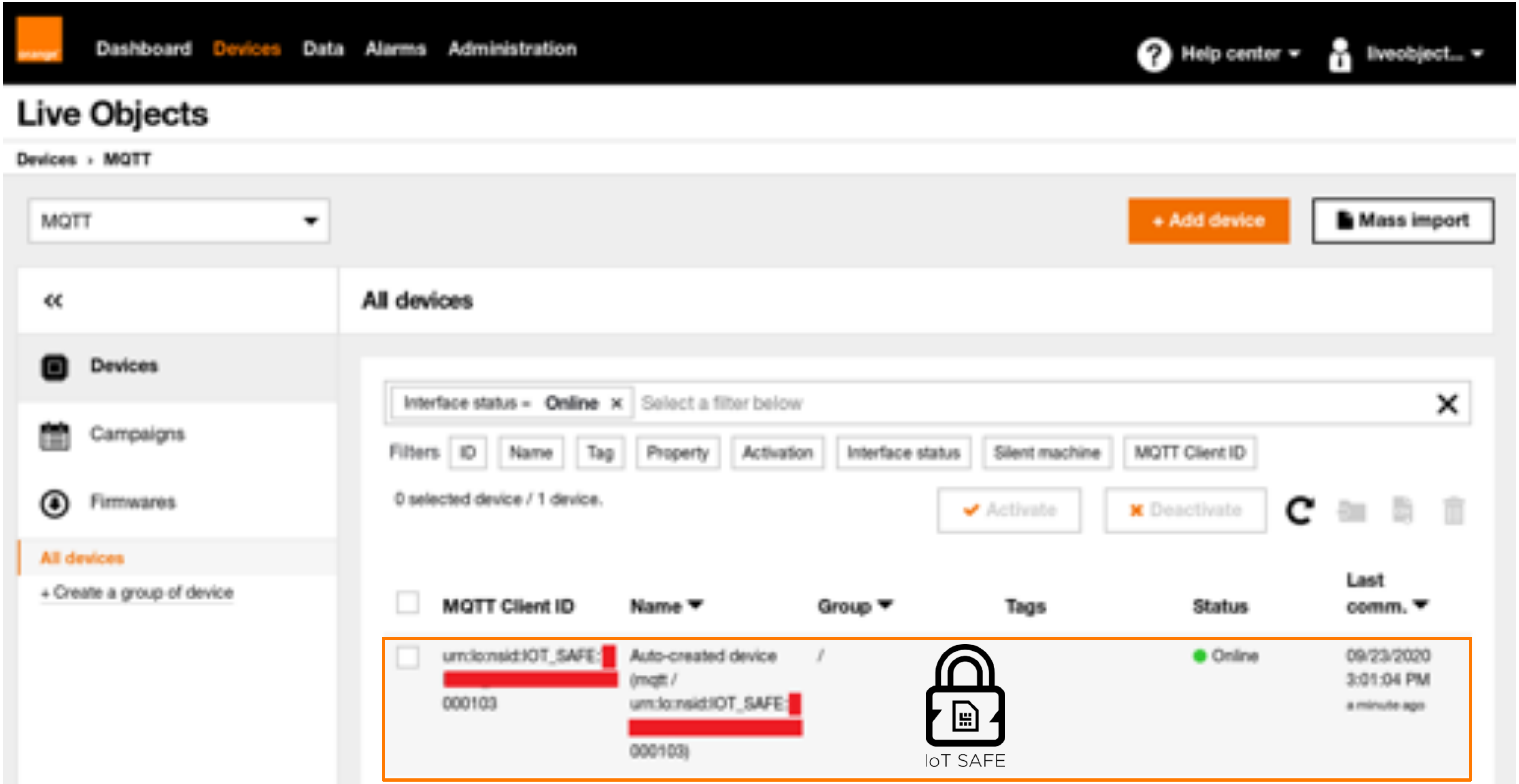
```
br_x509_certificate br_client_certificate =
  iotSAFE.readClientCertificate(IOT_SAFE_CLIENT_CERTIFICATE_FILE_ID,
    sizeof(IOT_SAFE_CLIENT_CERTIFICATE_FILE_ID));
sslClient.setEccCert(br_client_certificate);
sslClient.setEccSign(iot_safe_sign);
```

- Define the callback to offload the signature operation to the IoT SAFE applet (using a key ID or a label)



```
size_t iot_safe_sign(const br_ec_impl *impl, const br_hash_class *hf,
  const void *hash_value, const br_ec_private_key *sk, void *sig)
{
  return iotSAFE.sign(IOT_SAFE_PRIVATE_KEY_ID, sizeof(IOT_SAFE_PRIVATE_KEY_ID),
    impl, hf, hash_value, sk, sig);
}
```

Next Gen IoT Starter Kits: mTLS successful !



Live Objects

Devices › MQTT

MQTT

All devices

Interface status = Online × Select a filter below

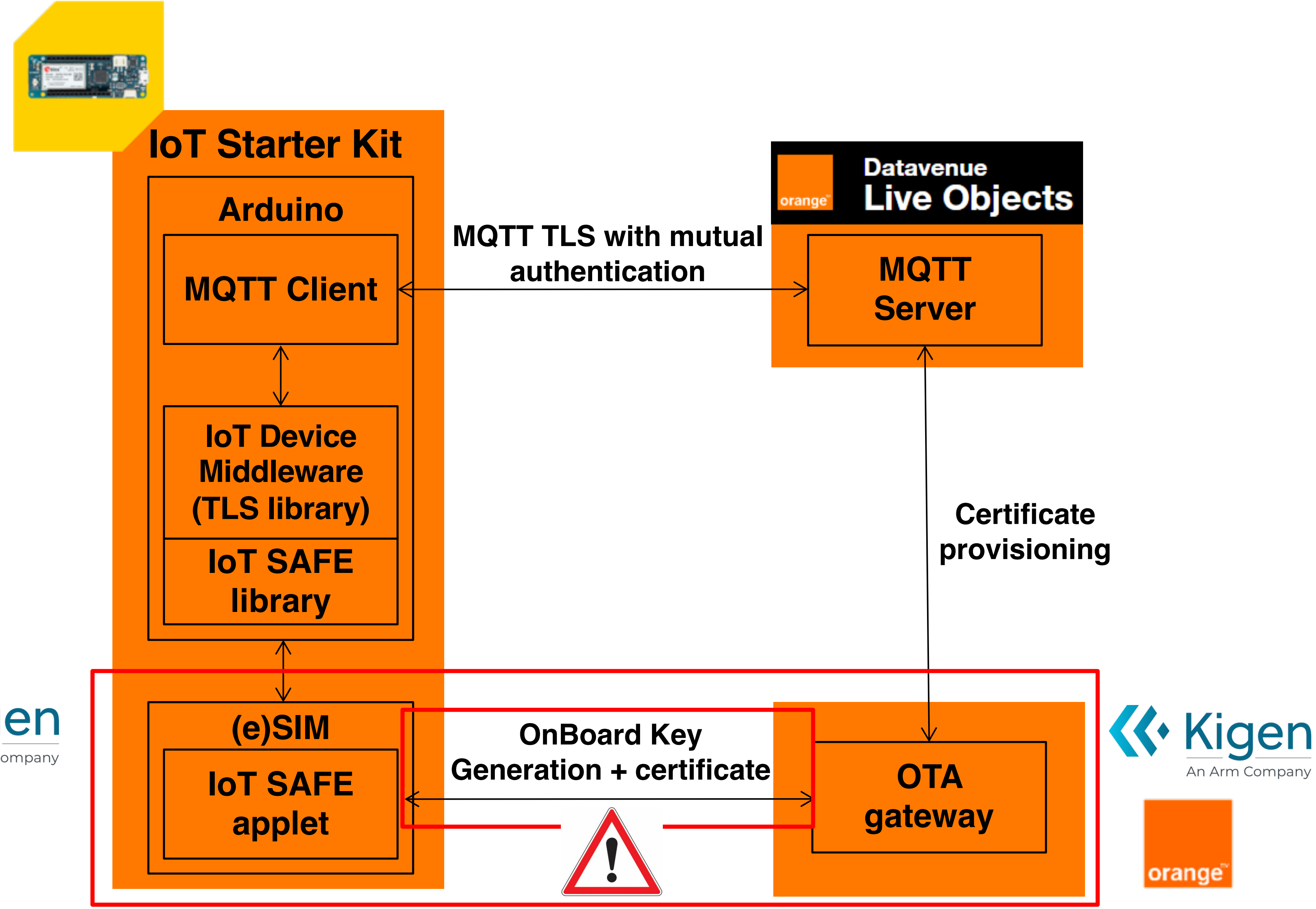
0 selected device / 1 device.

MQTT Client ID	Name	Group	Tags	Status	Last comm.
urn:lo:nsid:IOT_SAFE:[redacted] 000103	Auto-created device (mqtt / urn:lo:nsid:IOT_SAFE:[redacted] 000103)	/		● Online	09/23/2020 3:01:04 PM a minute ago

On the way to the next steps

Next Gen IoT Starter Kits: next steps

- Prototype the 2nd IoT SAFE scenario (on-board key generation) using our own OTA gateway or Kigen OTA
- Avoid any interoperability or proprietary lock down on the OTA interface
- Integrate IoT SAFE into release versions of major TLS stacks



Powering IoT innovation across the value chain

1. iSIM is a major catalyst for cellular LPWAN
2. IoT SAFE powers scalable enterprise-grade trust
3. Combined they're a winning combination & JavaCard technology is a key enabler for interoperability
4. IoT SAFE allows operators to remotely provision cloud credentials and keep them SECURE

Kigen

orange™

Questions?

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
תודה