Oracle Groundbreakers

IoT Secure Sensors Payload & Cloud Connection

Cristian Toma
Software Engineer
Oracle - Java Platform Group

Vlad Petrovici
Software Engineer
Oracle - Java Platform Group

December 2020

ORACLE

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Agenda

Overview

Demos Components and Java Card

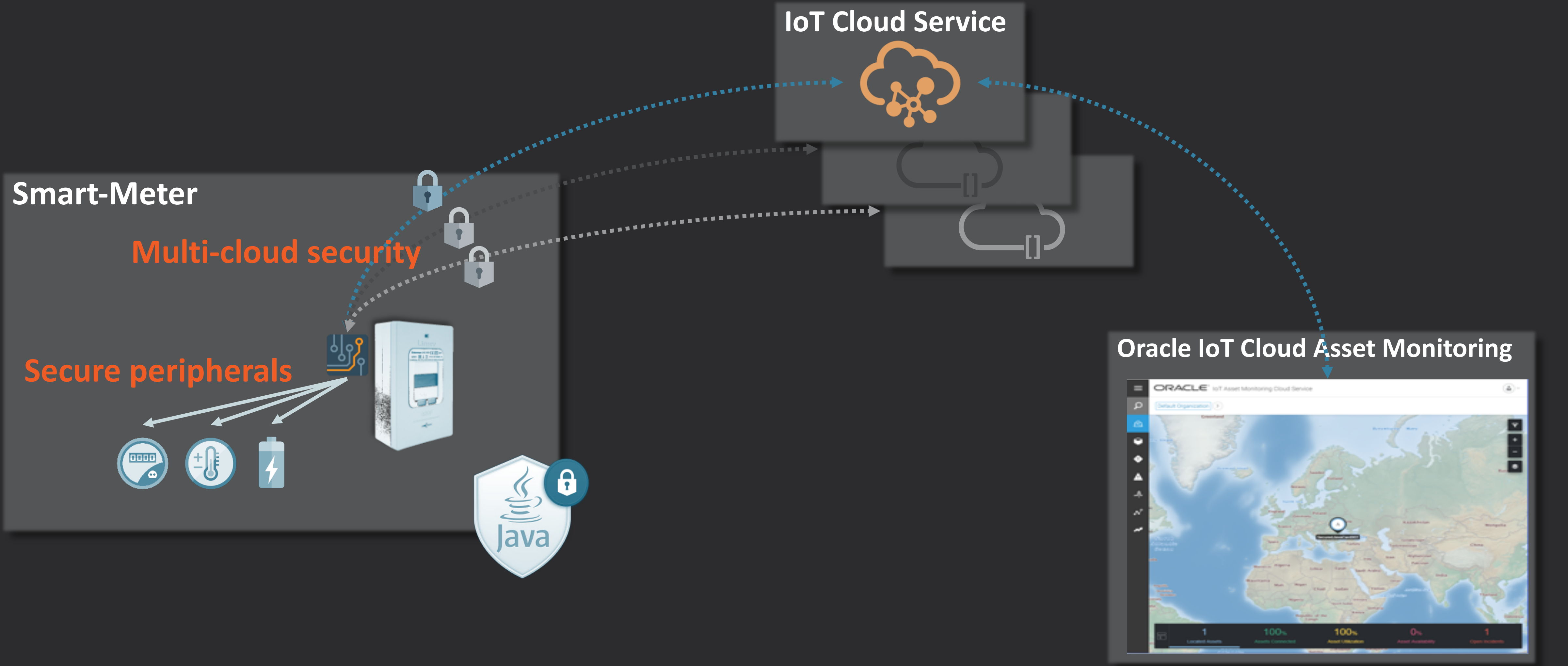
Demos Architecture & Data Flow

Conclusion

Agenda

- Overview
- Demos Components and Java Card
- Demos Architecture & Data Flow
- Conclusion

Overview



IoT Cloud Service

Smart-Meter

Multi-cloud security

Secure peripherals

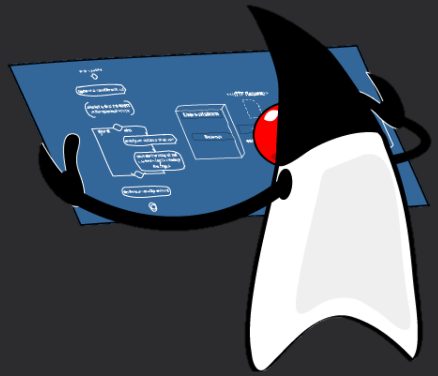
Oracle IoT Cloud Asset Monitoring

Demos

- ***IoT Secure Peripherals Demo***
  - Java Card platform extensions to support specific I/O communication with peripherals
  - Application within secure element directly controlling and accessing peripherals

- ***IoT Multi-Cloud Security Demo***
  - Device enrollment/on-boarding
  - Secure IoT Cloud Authentication and Authorization
  - Multi IoT Solution Providers support

Agenda



Overview

➡ Demos Components and Java Card

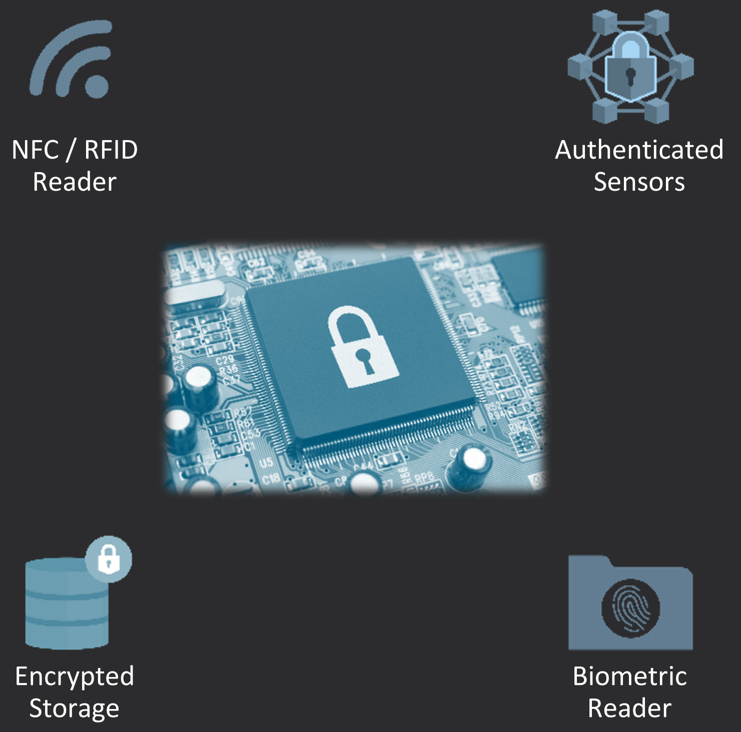
Demos Architecture & Data Flow

Conclusion

Java Card Secure Peripherals

Secure the “last yard” between devices and attached peripherals, enabling trust and exchange of sensitive data at the very edge.

- Secure Channel between peripherals and security chip
- Authenticated data sources at the edge
- Out of band communication for sensitive data (biometric info, root of trust credentials)
- Encrypted Data Storage



NFC / RFID Reader

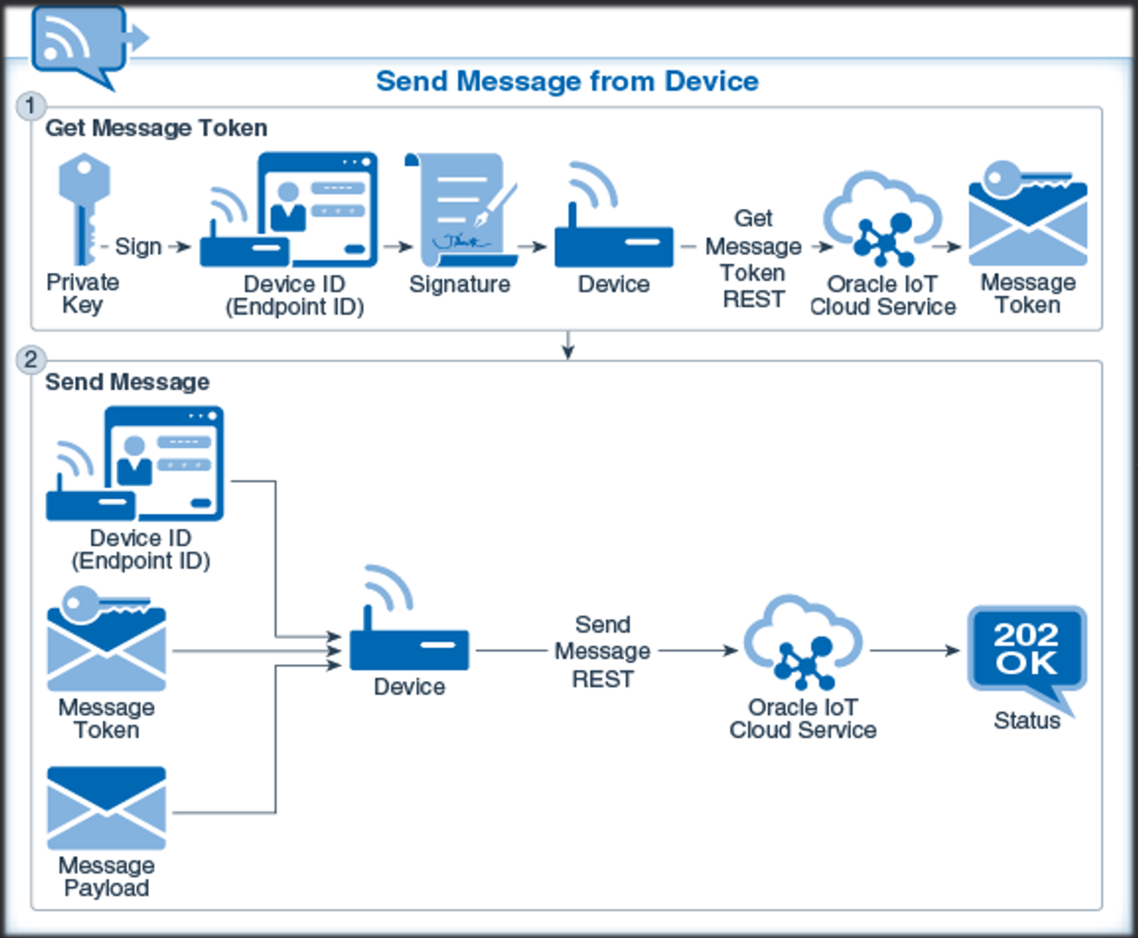
Authenticated Sensors

Encrypted Storage

Biometric Reader

Java Card enabling Multi-Cloud Authentication Schemes

Oracle IoT CS – RSA with SHA-256



Send Message from Device

1 Get Message Token

Private Key – Sign → Device ID (Endpoint ID) → Signature → Device – Get Message Token REST → Oracle IoT Cloud Service → Message Token

2 Send Message

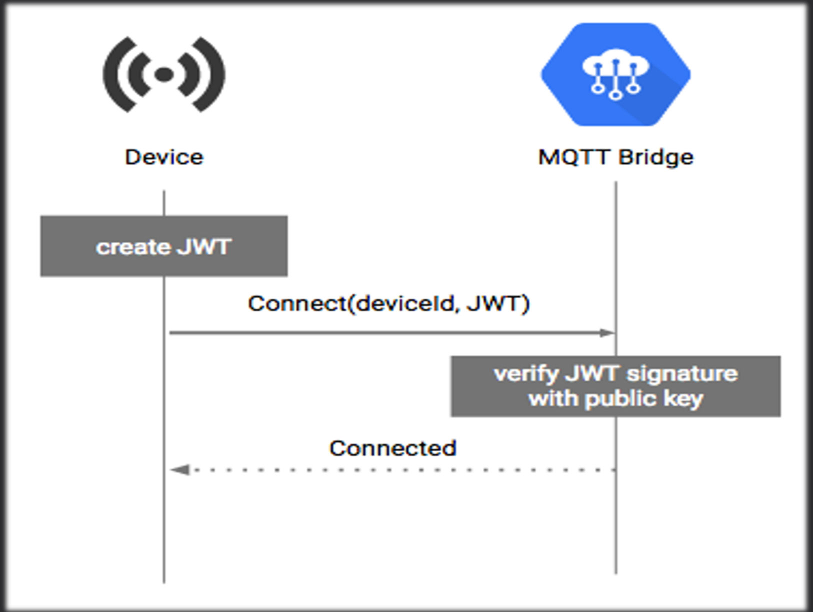
Device ID (Endpoint ID)

Message Token

Message Payload

Device – Send Message REST → Oracle IoT Cloud Service → 202 OK Status

Java Card



Device

MQTT Bridge

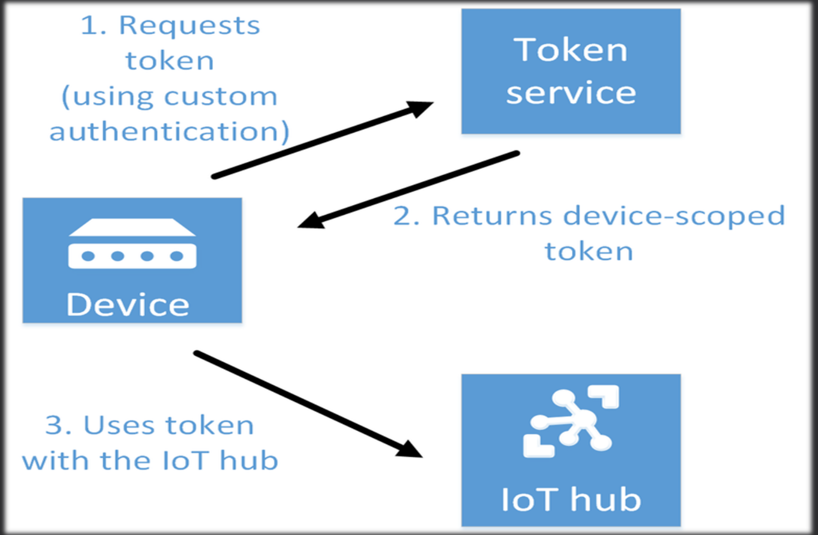
create JWT

Connect(deviceId, JWT)

verify JWT signature with public key

Connected

Google IoT Pub-Sub – RSA / ECDSA with SHA-256



1. Requests token (using custom authentication)

Token service

2. Returns device-scoped token

Device

3. Uses token with the IoT hub

IoT hub

MS IoT Azure Hub – TLS 1.3 Authentication

Java Card 3.1 Features for IoT

- **Certificate API** to optimize storage and certificate handling
- **Key derivation API** for secure communications
- **Monotonic Counter API** for anti-replay functions
- **System Time API** for timestamps or watchdogs

- **Extended File Format** for modular and large applications
- **Array views** for efficient sharing
- **Static resources** for applications configuration
- Improved capabilities for **API upgrade**

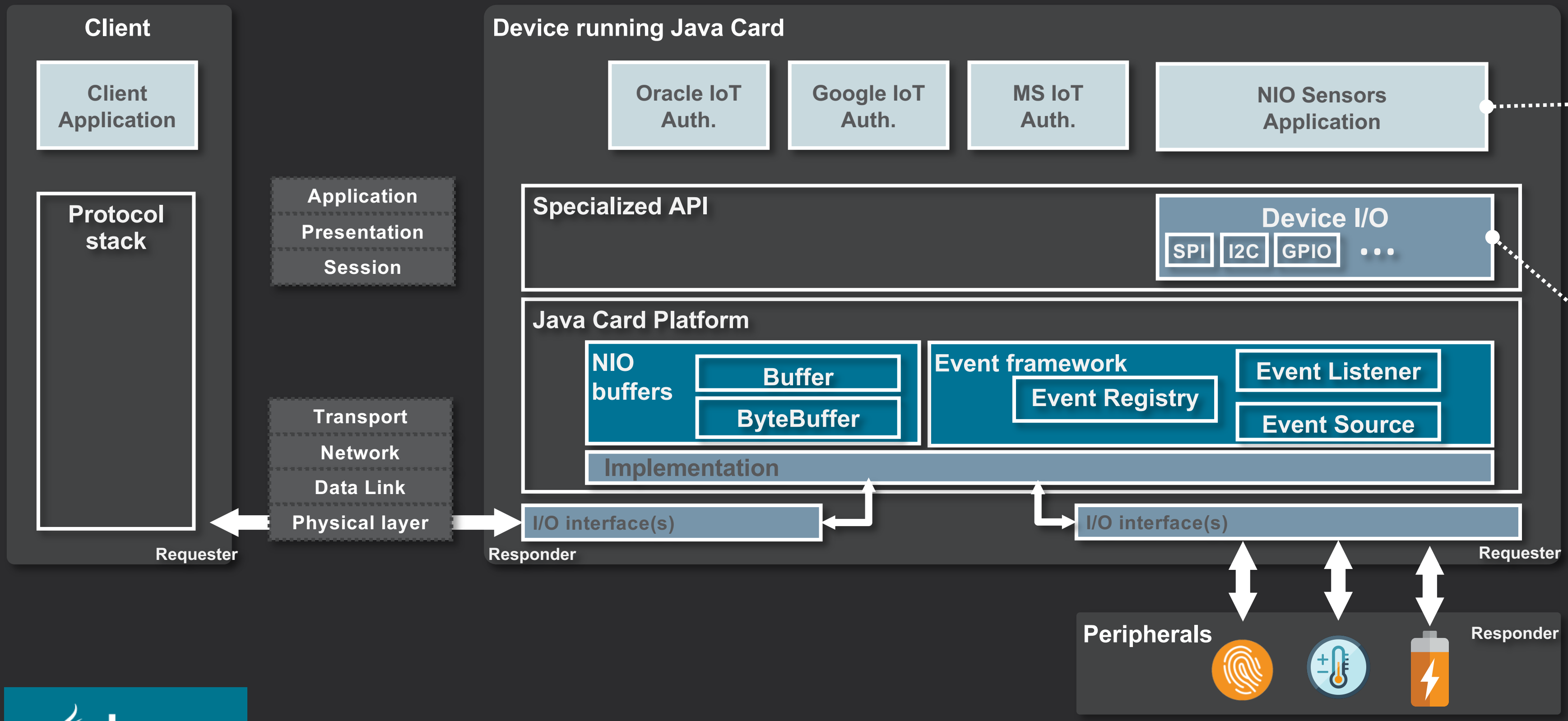
- **Extensible I/O framework** to support new physical interfaces and access peripherals
- **I/O Buffers** for efficient data handling

- **Enhanced Elliptic Curves Cryptography** with new curves
- **Configurable Key Pair generation** for better control on key generation
- **New cryptographic algorithms**

Extensible I/O Framework enabling secure sensors

API exposing physical I/O interfaces

for application developers to access peripherals or I/O interfaces and develop their own protocols



Applications can access I/O

- To develop custom protocols
- To access peripherals

Device I/O API

- Device interface, open, configure
- Specific classes for SPI, I2C, GPIO …

▭	Application developer
▨	Platform implementer
■	Java Card 3.1 API

Agenda

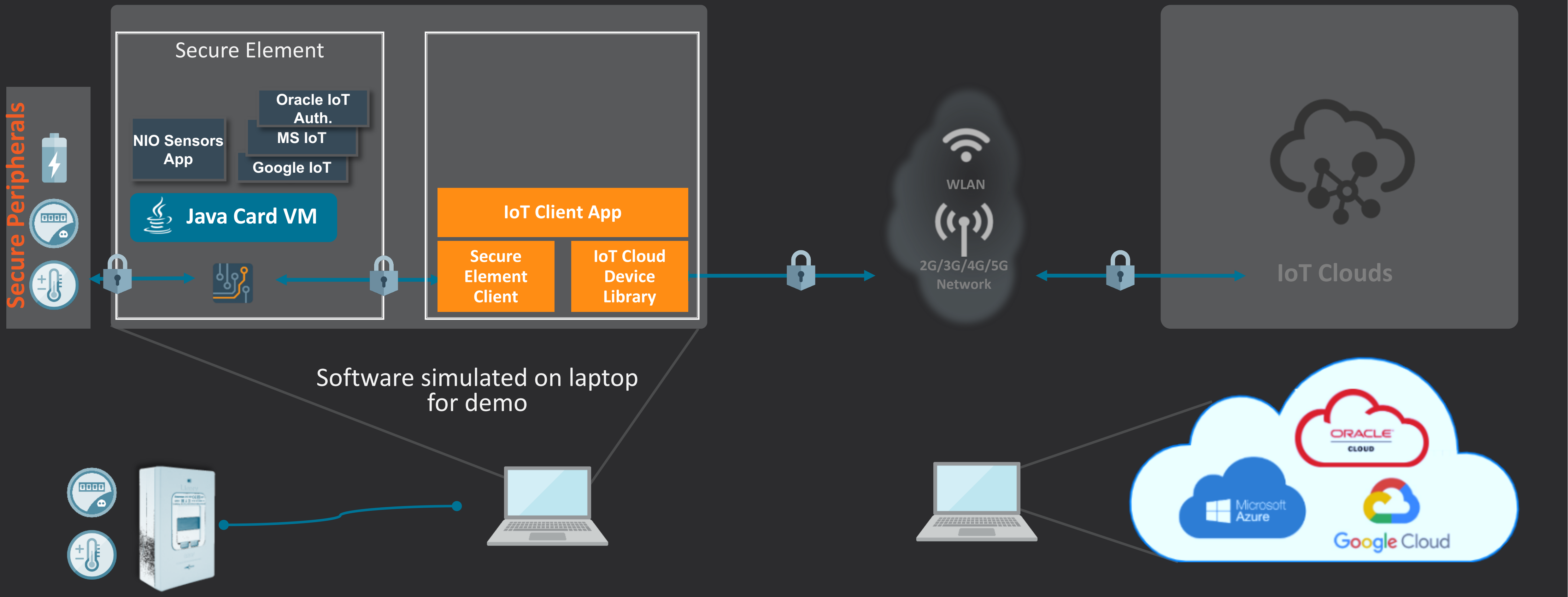
Overview

Demos Components and Java Card

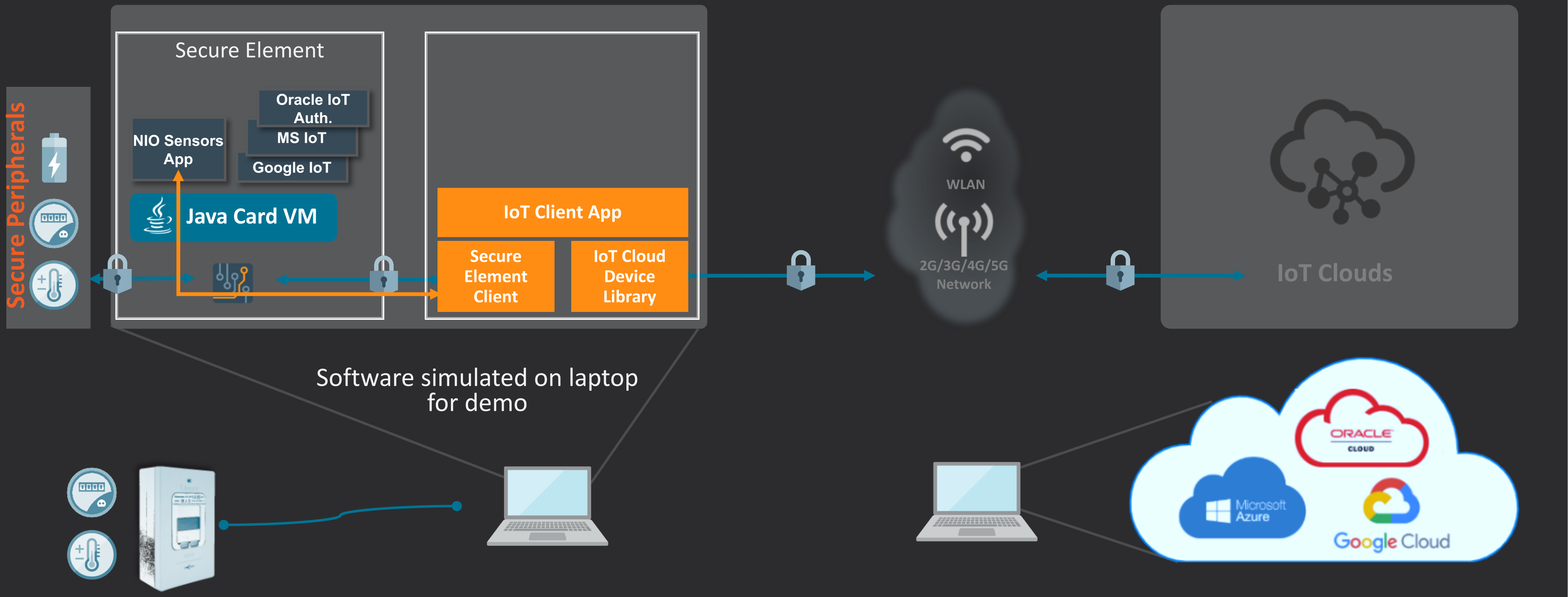
➡ **Demos Architecture & Data Flow**

Conclusion

Demo architecture

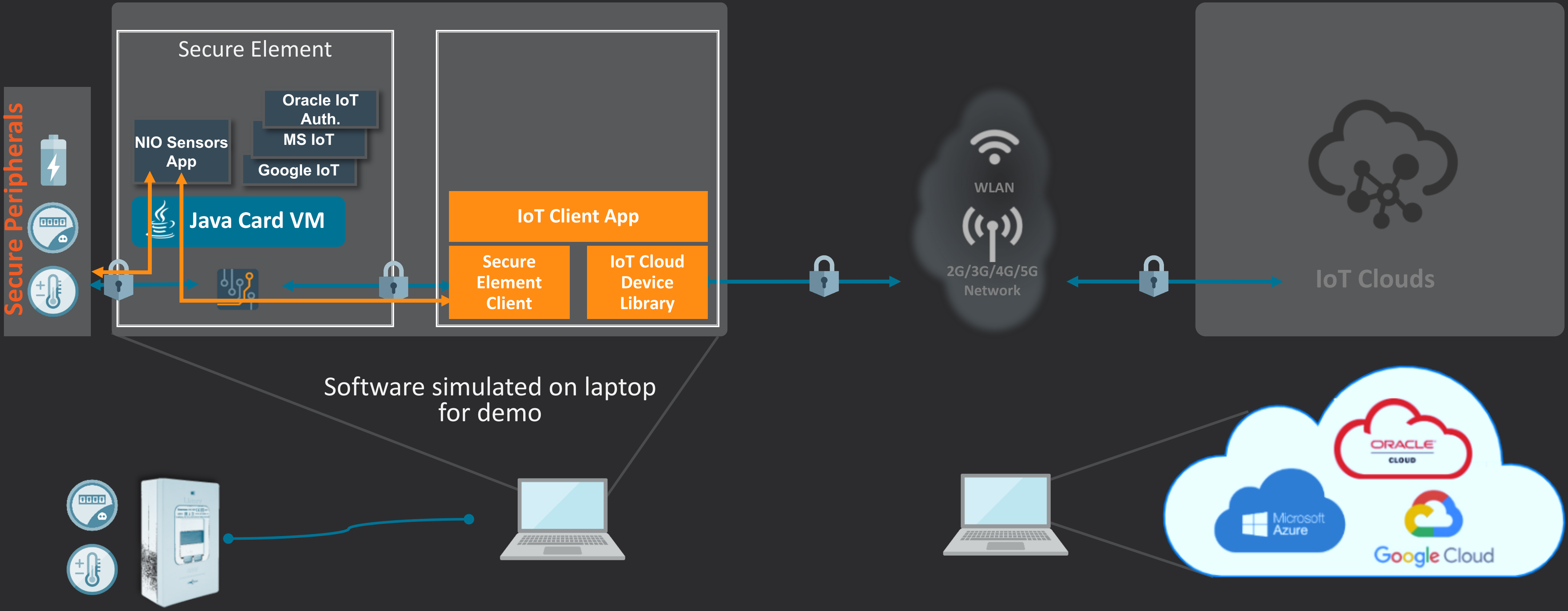


Demo architecture

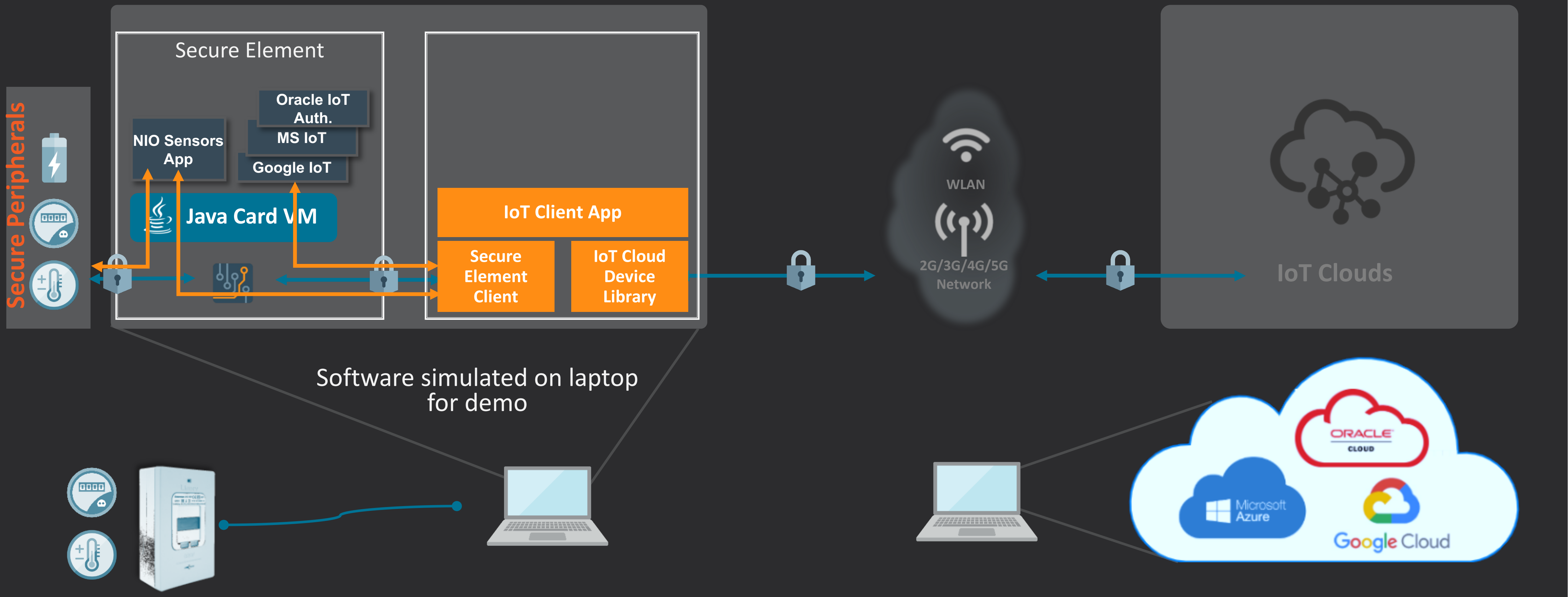


Software simulated on laptop for demo

Demo architecture

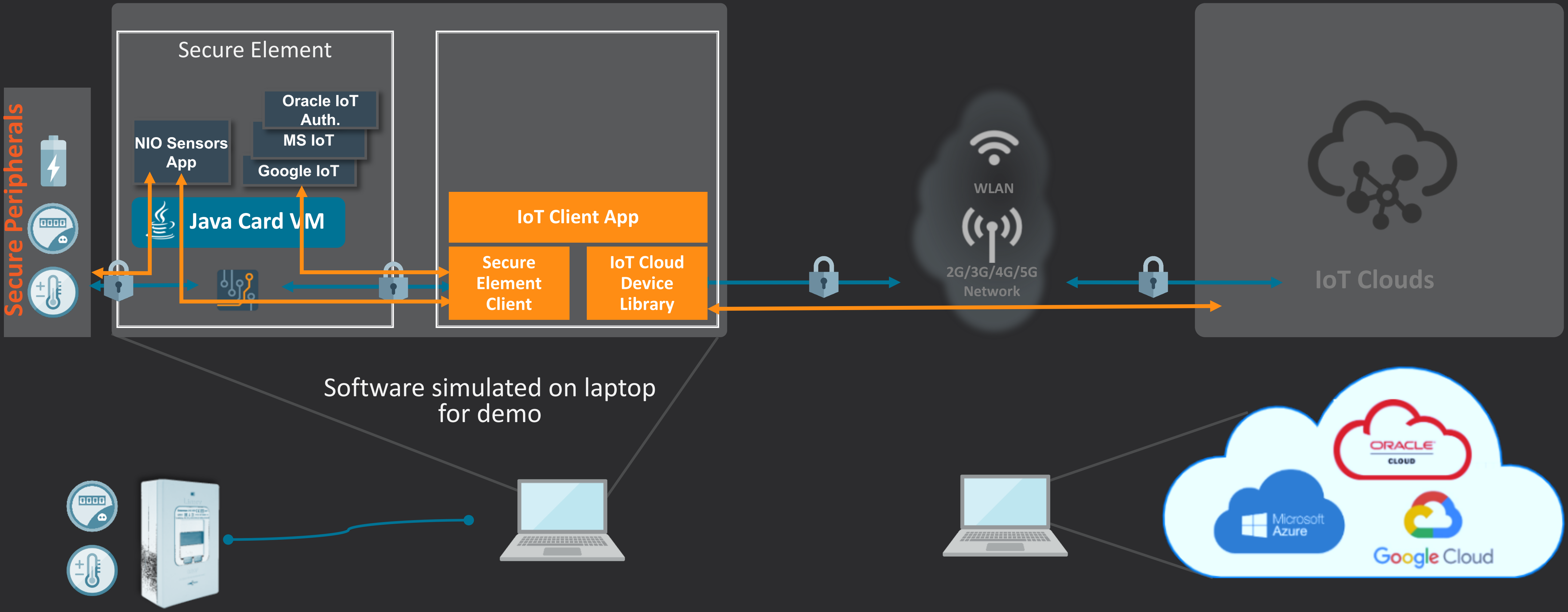


Demo architecture



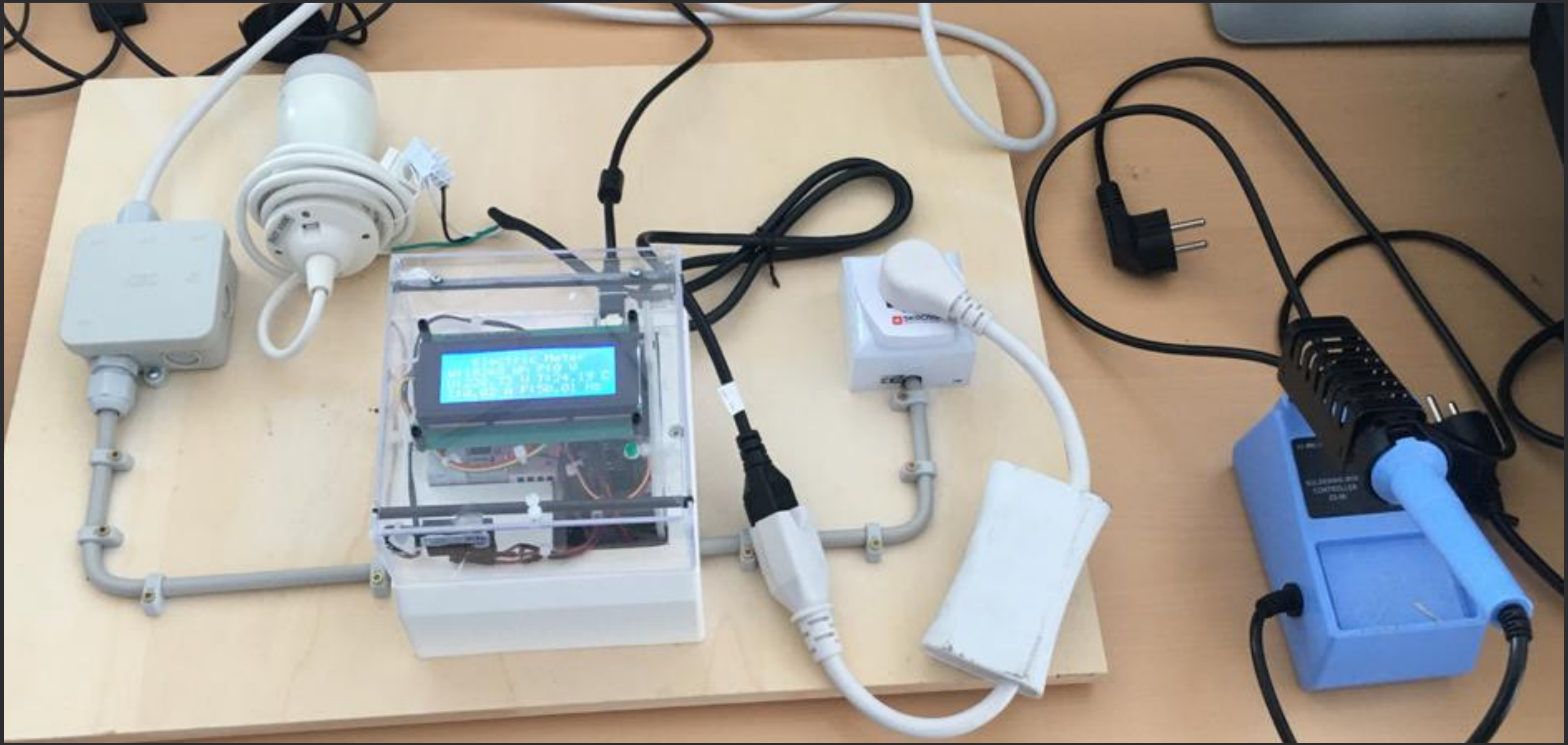
Software simulated on laptop for demo

Demo architecture

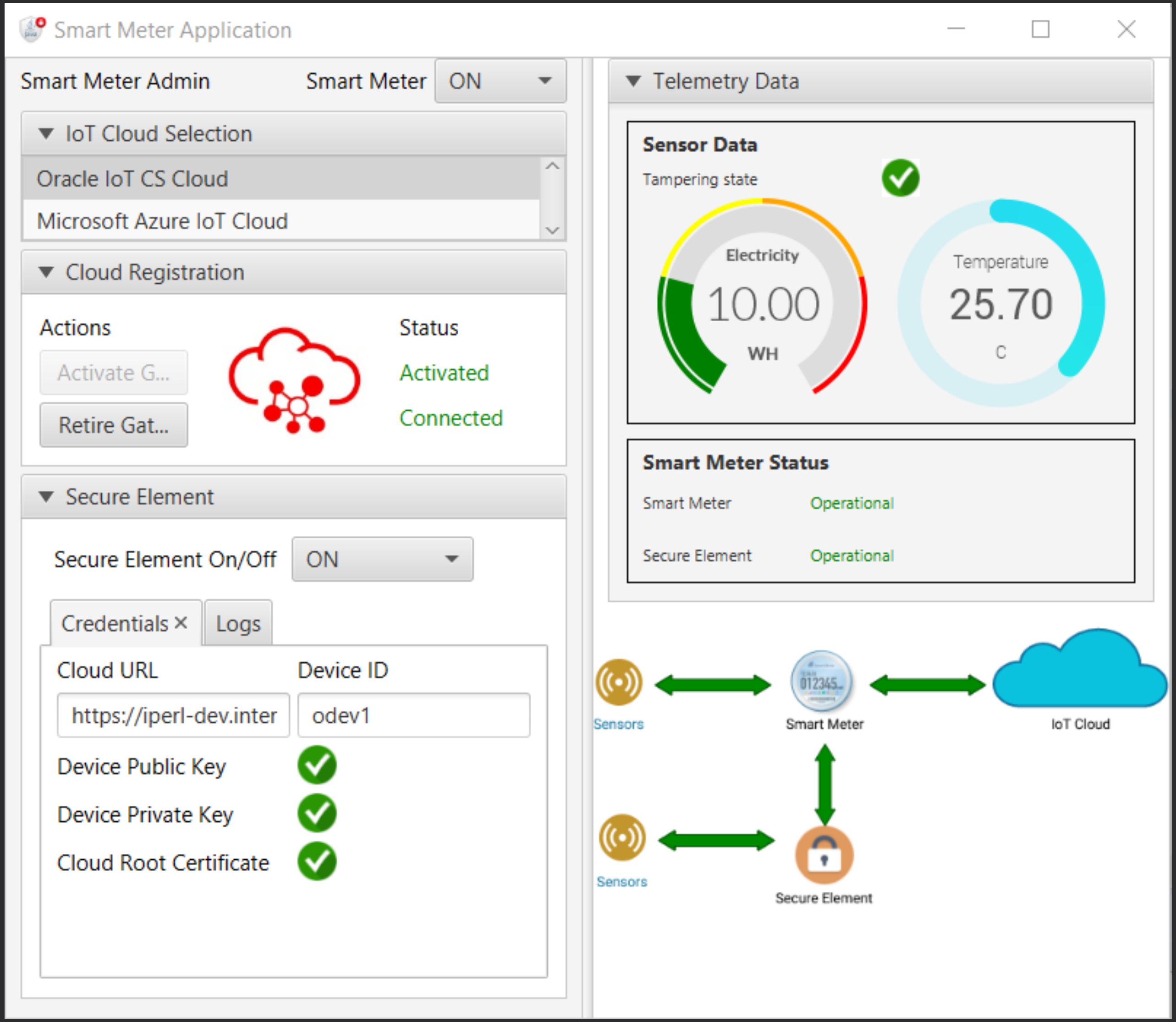


Software simulated on laptop for demo

Demo HW components Setup



Smart Meter Monitoring Tool Application



Smart Meter Application

Smart Meter Admin

Smart Meter: ON

IoT Cloud Selection

- Oracle IoT CS Cloud
- Microsoft Azure IoT Cloud

Cloud Registration

Actions	Status
Activate G...	Activated
Retire Gat...	Connected

Secure Element

Secure Element On/Off: ON

Credentials × | Logs

Cloud URL	Device ID
https://iperl-dev.inter	odev1

Device Public Key ✓

Device Private Key ✓

Cloud Root Certificate ✓

Telemetry Data

Sensor Data

Tampering state ✓

Electricity 10.00 WH

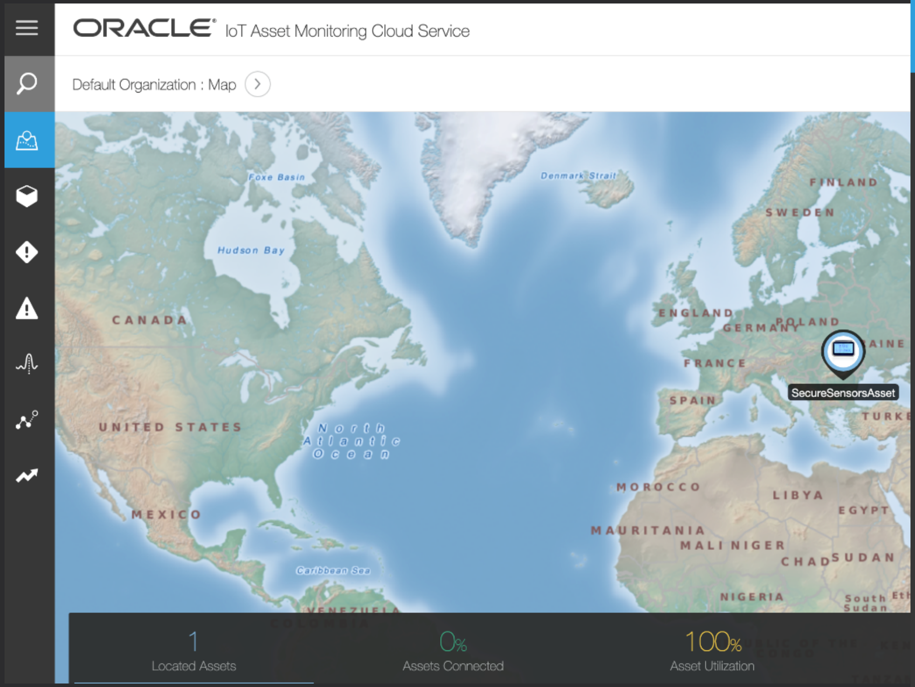
Temperature 25.70 C

Smart Meter Status

Smart Meter: Operational

Secure Element: Operational

Oracle IoT Cloud Asset Monitoring



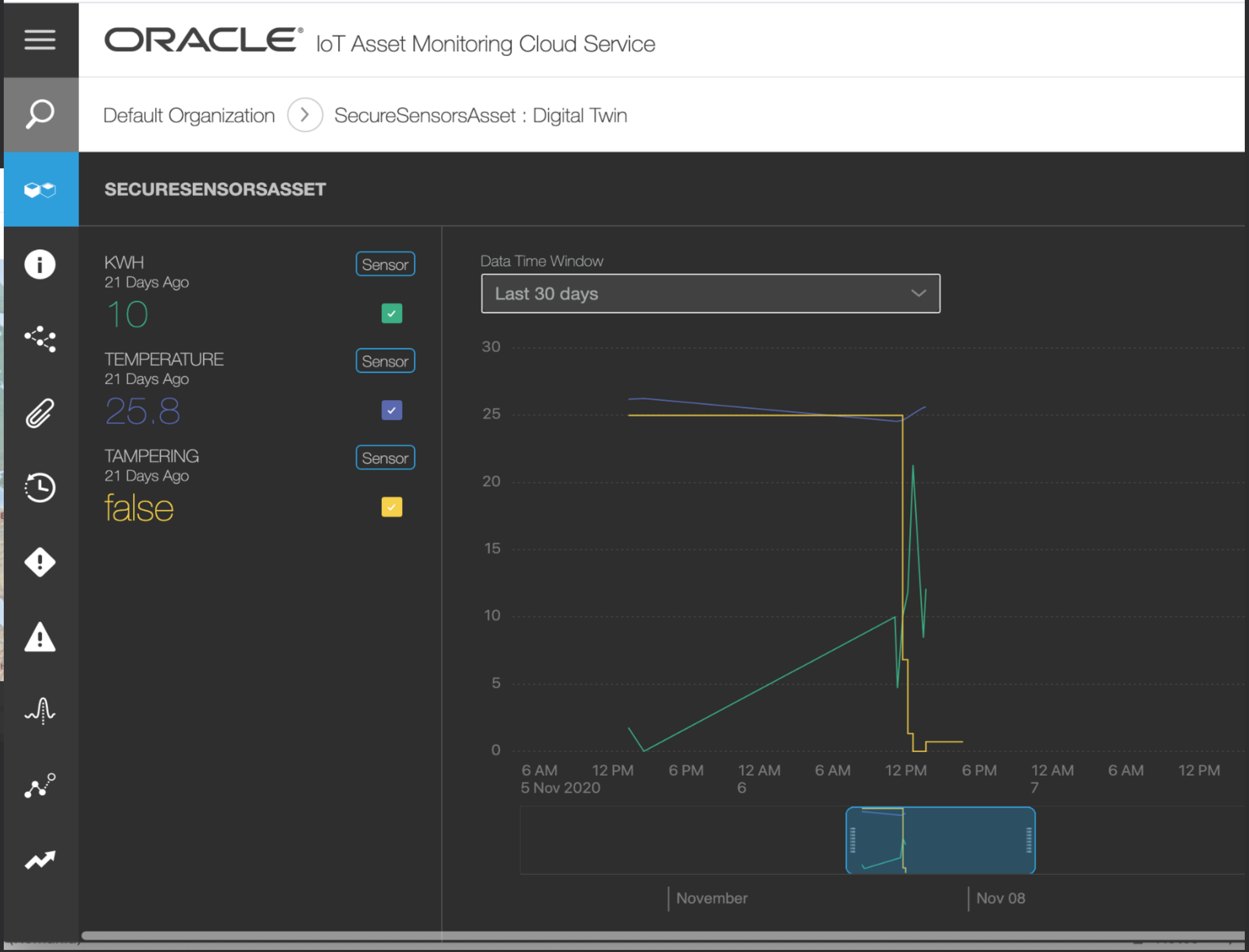
ORACLE IoT Asset Monitoring Cloud Service

Default Organization : Map

1 Located Assets

0% Assets Connected

100% Asset Utilization



ORACLE IoT Asset Monitoring Cloud Service

Default Organization > SecureSensorsAsset : Digital Twin

SECURESENSORSASSET

KWH
21 Days Ago
10
Sensor ✓

TEMPERATURE
21 Days Ago
25.8
Sensor ✓

TAMPERING
21 Days Ago
false
Sensor ✓

Data Time Window: Last 30 days

Agenda

Overview

Demos Components and Java Card

Demos Architecture & Data Flow

➡ **Conclusion**

Secure Peripherals and IoT Multi-Cloud Connection using Java Card

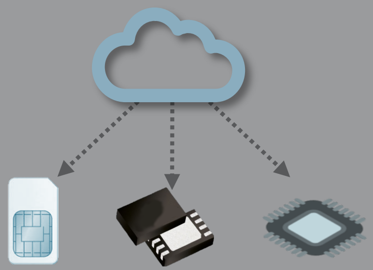
Conclusion

Secure Runtime

- To securely store and manage crypto keys for IoT Cloud Authentication
- To run the cryptographic algorithms in the Secure Element: create tokens, encrypt and sign the payload

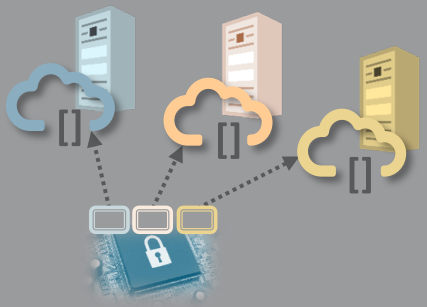
Portable

- To address the highly fragmented IoT landscape
- To deploy and operate the secure applications – Java Card Applets on multiple hardware platforms, from different vendors



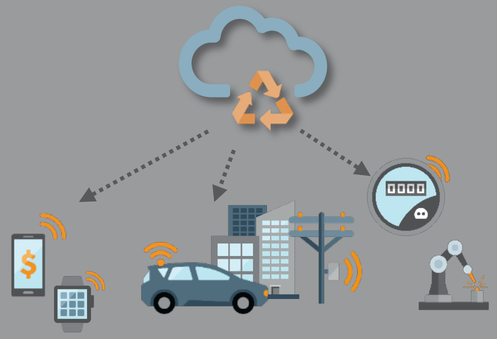
Adaptable & Extensible

- To support multiple authentication schemes and IoT Clouds
- To enable payload handling from different peripherals using various protocols



Manageable

- To update and upgrade the Java Card applets and remaining compliant with the fast evolving security requirements and regulations



More Information

https://www.oracle.com/java/technologies/java-card-tech.html

Java Card Platform Specification 3.1

Latest release of the Java Card specification and the reference for Java Card products.

Java Card Development Kit Tools

The Java Card Development Kit Tools are used to convert and verify Java Card applications. The Tools can be used with products based on version 3.1, 3.0.5 and 3.0.4 of the Java Card Specifications.

Java Card Development Kit Simulator

The Java Card Development Kit Simulator includes a simulation component and Eclipse plug-in.
Combined with the Java Card Development Kit Tools, it provides a complete, stand-alone development environment.

Java Card IoT and Security blog

This Blog covers the latest Java technology for small devices and security in the IoT, mobile, ID and Payment.

Webcast – Secure Business Runs Java Card

Webcast – How to secure IoT Edge with Java Card

Webcast: Oracle Java Card 3.1 Boosts Security for IoT Devices at the Edge

contacts: cristian.v.toma at oracle dot com, vlad.petrovici at oracle dot com