

Date 26th February 2020

IoT SAFE

Enabling a profitable and sustainable connected business

co-Presenters Kudelski Group and u-blox AG / GSMA MWC 2020

Who are we?

Two trusted, experienced partners based in Switzerland:

Kudelski Group

- Leader in securing digital content, cybersecurity, and public access solutions
- 30+ years **securing** high-value business models and **defending** them against criminal and state-agent attacks



\$100B

revenue enabled annually

400+ M

devices secured

Swiss Exchange
listed

u-blox AG

- Leader in low-power wide-area, cellular technologies
- 20+ years connecting and positioning M2M and IoT devices



6000 customers

Full IP for
LPWA

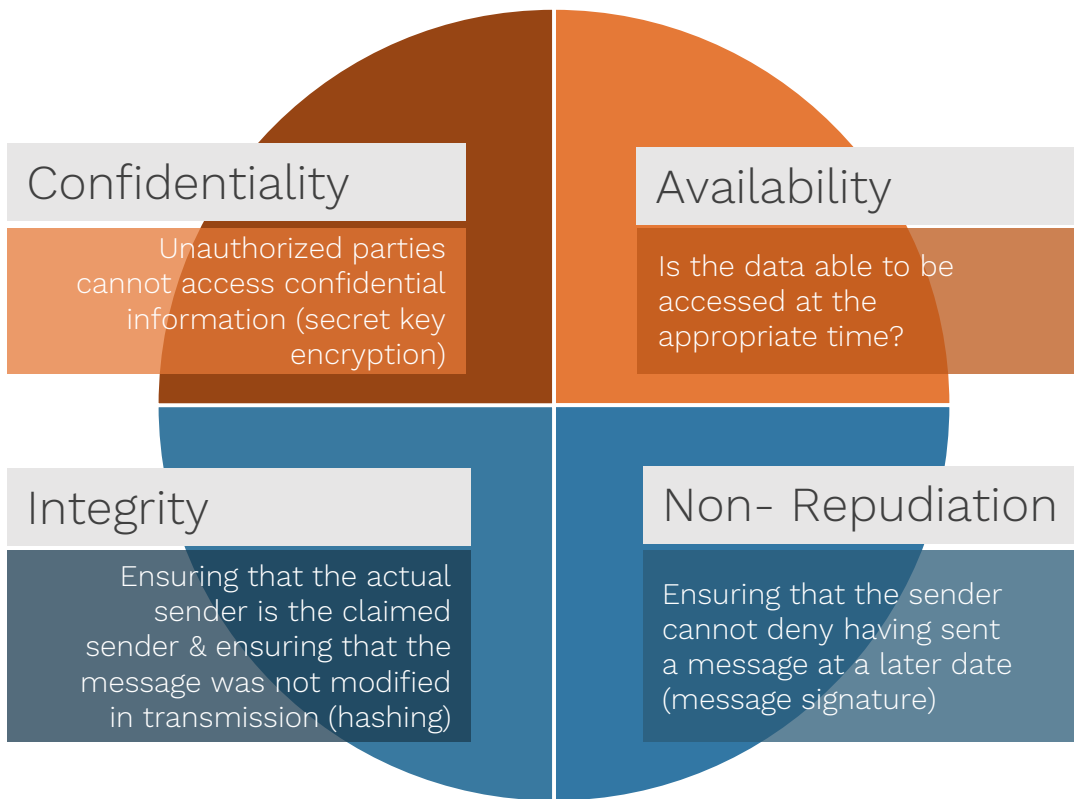
Swiss Exchange
listed

End-to-end data security

Secure IoT ecosystems require optimized

IoT Key Management

that ensure:





Good security requires

Robustness to attacks

Logical attacks – e.g. software fuzzing

Side channel attacks (SCA) – DPA etc.

Fault injection attacks (DFA)
– Laser / EMC glitching

Tamper resistant hardware makes sense

And is available in all GSMA IoT devices
in the form of common criteria

EAL4/5+ **SIM cards / Secure Elements.**

Optimized Trust for low power networks

Symmetric
mode to reduce
power &
bandwidth

Shared keys
without
exchange

Power Efficiency

Easy »at scale»
Key Management &
disaster recovery

Avoid losing
millions of device
keys

Scalability

Enable remote
management of
deployed solution

Updates for
security and
functionality

Renewability

Optimized Trust for low power networks

Robust & Scalable IoT Key Management

- ✓ Rotate and replace keys frequently
- ✓ Never expose these keys outside the secure environment
- ✓ Derive Keys from RoT for security functions
- ✓ Generate trusted identity and mutual authentication
- ✓ Provision immutable RoT of Trust

Why use IoT SAFE?

- Leverages existing security hardware resources to securely store and manage keys
- Enables the remote management (cloud based) of deployed security applets (good security requires renewability).
- Enables Symmetric Key system that is optimized for IoT (Type II PSK)
- Standardized solution that runs on all GSMA networks
- Easy developments for device manufacturers; immutable identity is pre-provisioned in the SIM



*Note – Kudelski did not participate in GSMA nor in SIM Alliance but we developed our system internally

Securing IoT devices protects data and your business, with safety as paramount



Connected Hospital

Improve care and comply with regulations with connected systems that guarantee patient privacy and data integrity



Connected Patient

Ensure patient safety and base care decisions on trust via authentic, protected data that can be traced to the correct device



Remote Wellness Support

Improve efficiency via daily activity monitoring with personal devices that are robust to attacks

IoT data security in use

Typical approaches in securing communications

Typical PKI system



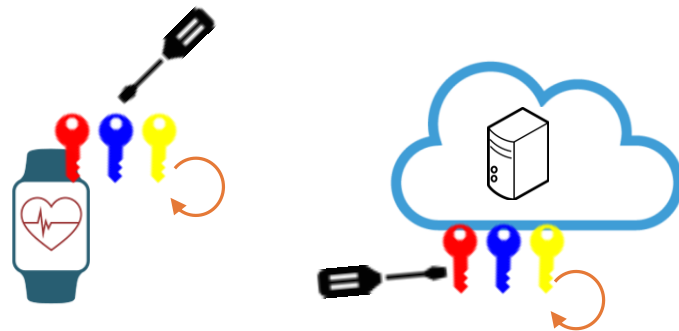
Must “know” the same CA

Certificates lifecycle management

Private keys and certificates securely generated on the server side, then securely delivered and protected

Inefficient on processing/handshaking

Typical PSK system



Must “know” each other

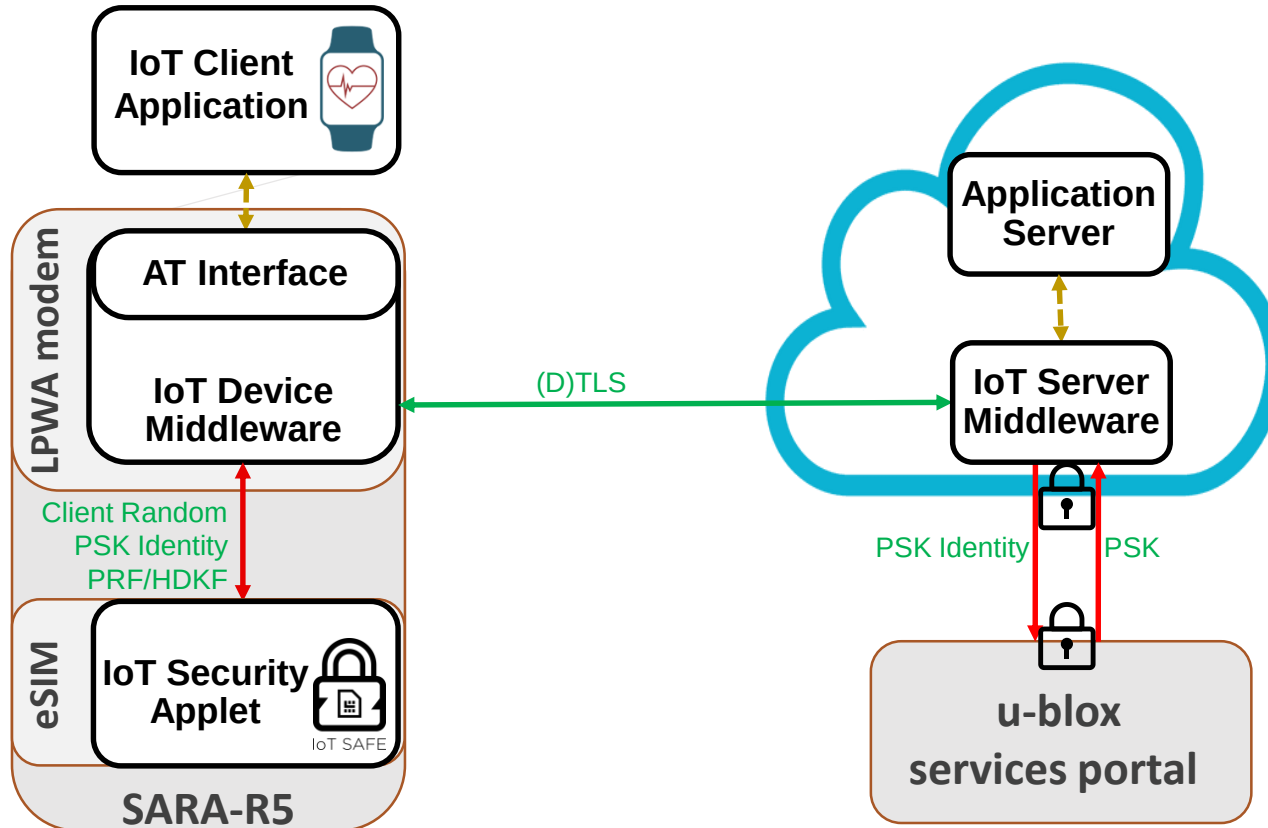
Secure channel needed to deliver key

PSK protection on client and on server

Requires a keys rotation solution

IoT SAFE data security in use

u-blox solution in partnership with Kudelski



- u-blox portal required only to check identity and retrieve your key
- Sensitive data never goes through u-blox servers
- Session Key can be used at any time and changed as you like

IoT SAFE business benefits

u-blox and Kudelski focus on customer success



- Easier to establish a (D)TLS session with an application cloud/server
- Entirely removes need for keys (PKI or PSK) management and delivery
- Simplifies the provisioning and managing of millions of IoT devices
- Optimizes energy budget by reducing data overhead and packet flights
- eSIM acts as a RoT and protects data at rest and in motion

Leikr
Advanced Sports Electronics