IoT connectivity / LoRa networks / Security

Nov 2015

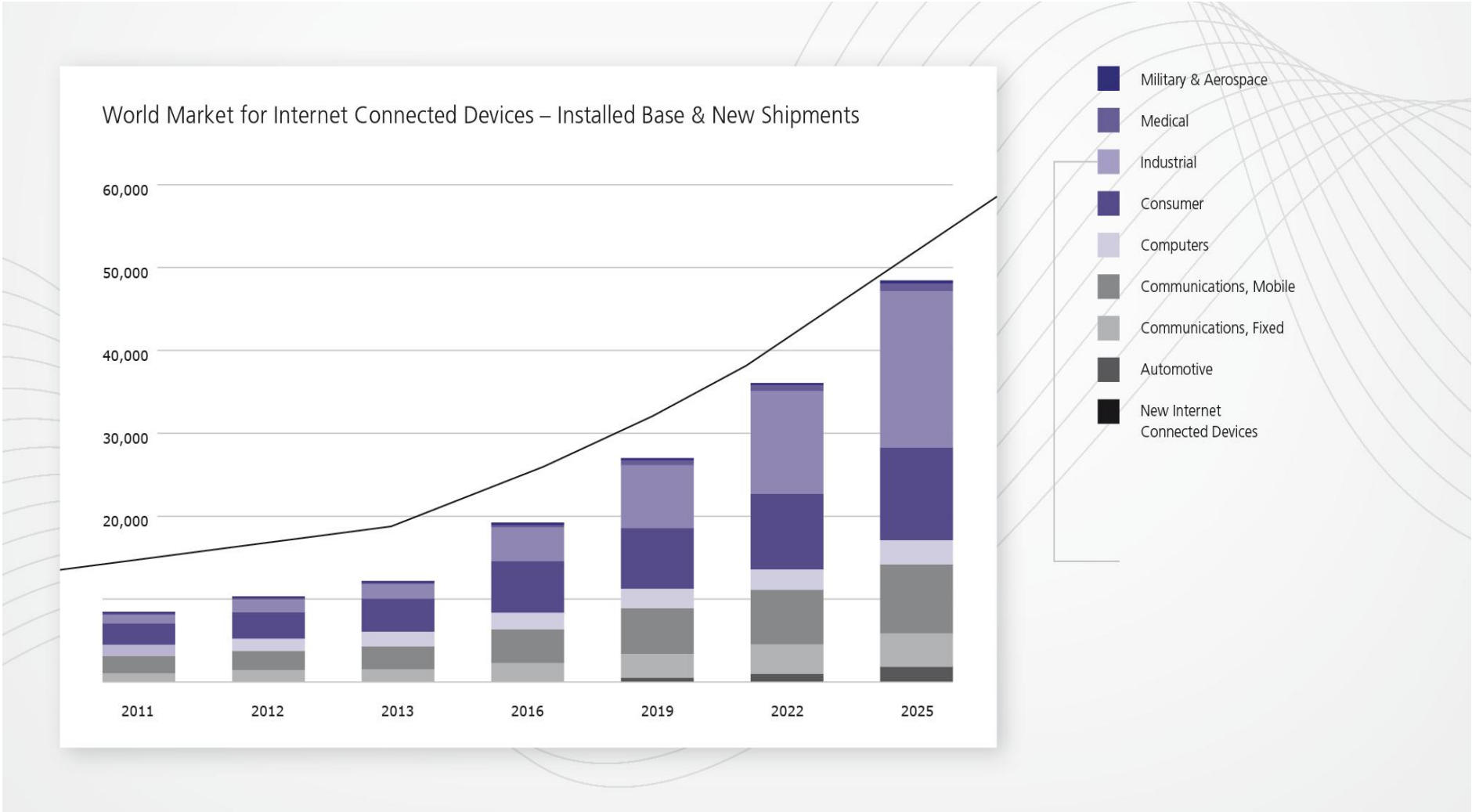
Accelerating Your Success™

What is IoT / M2M ?

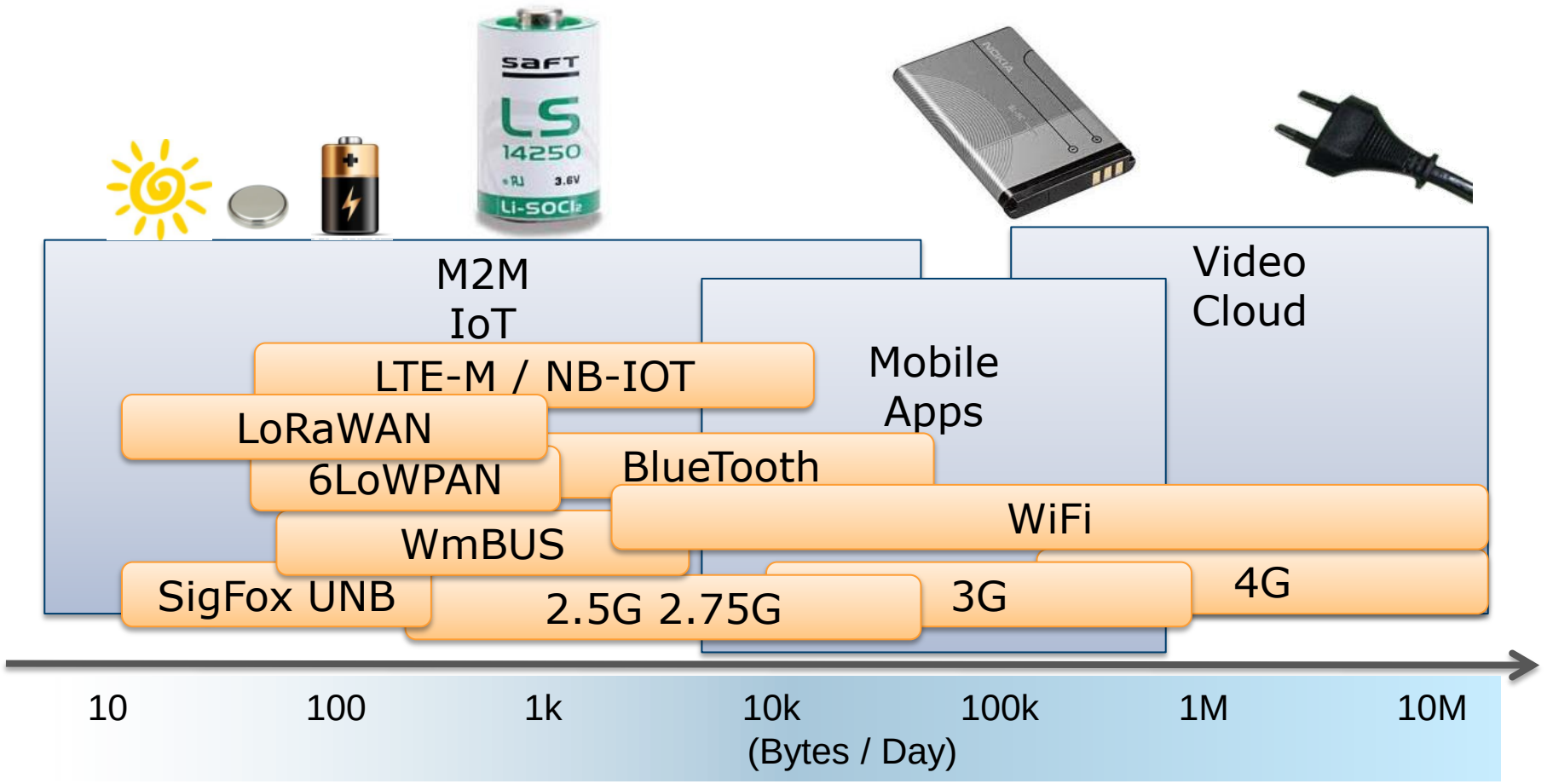
Internet of Things (IoT)

Machine to Machine (M2M)

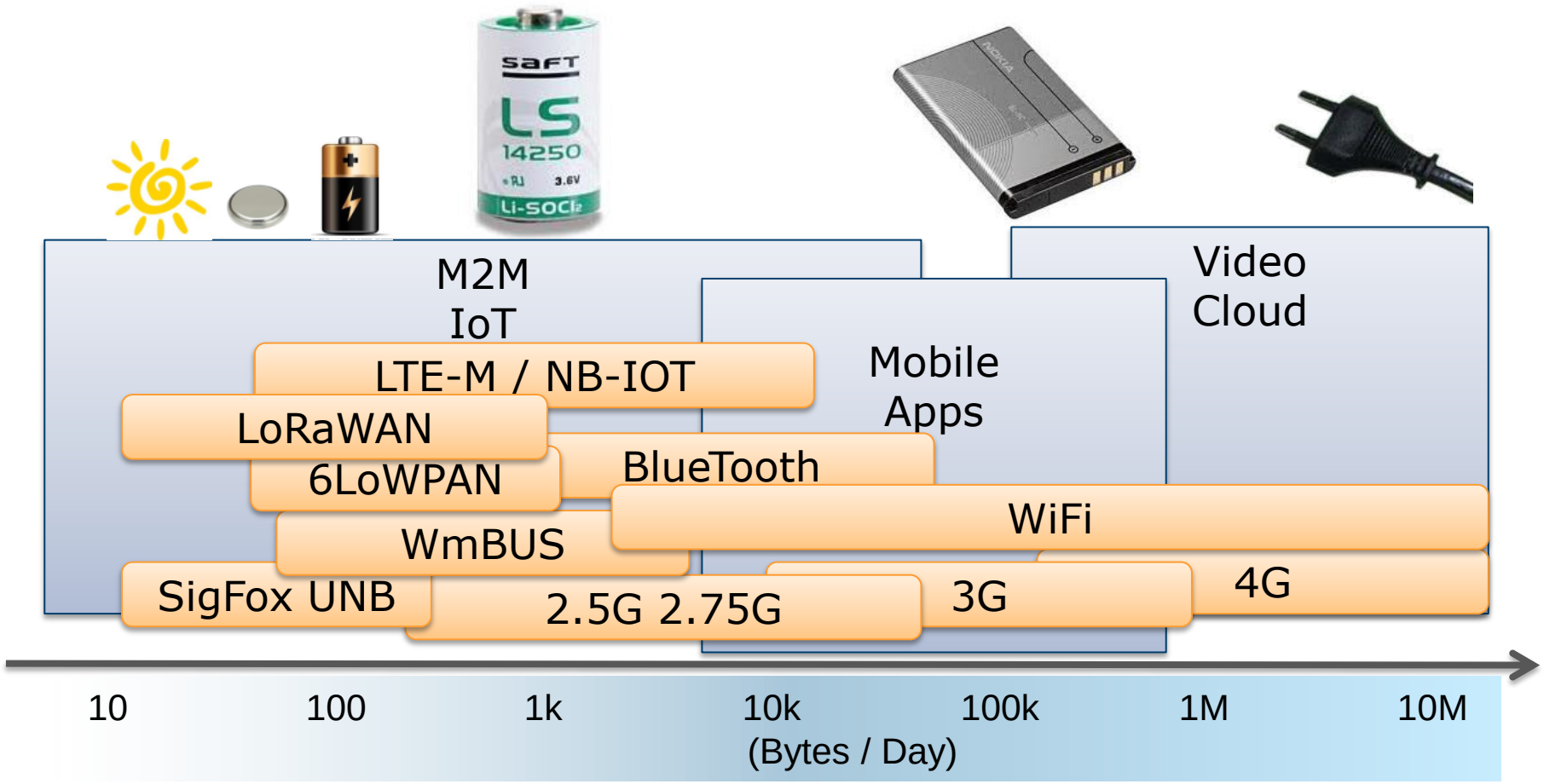
To Be connected or not to Be at all ?



Wireless – wireless – wireless



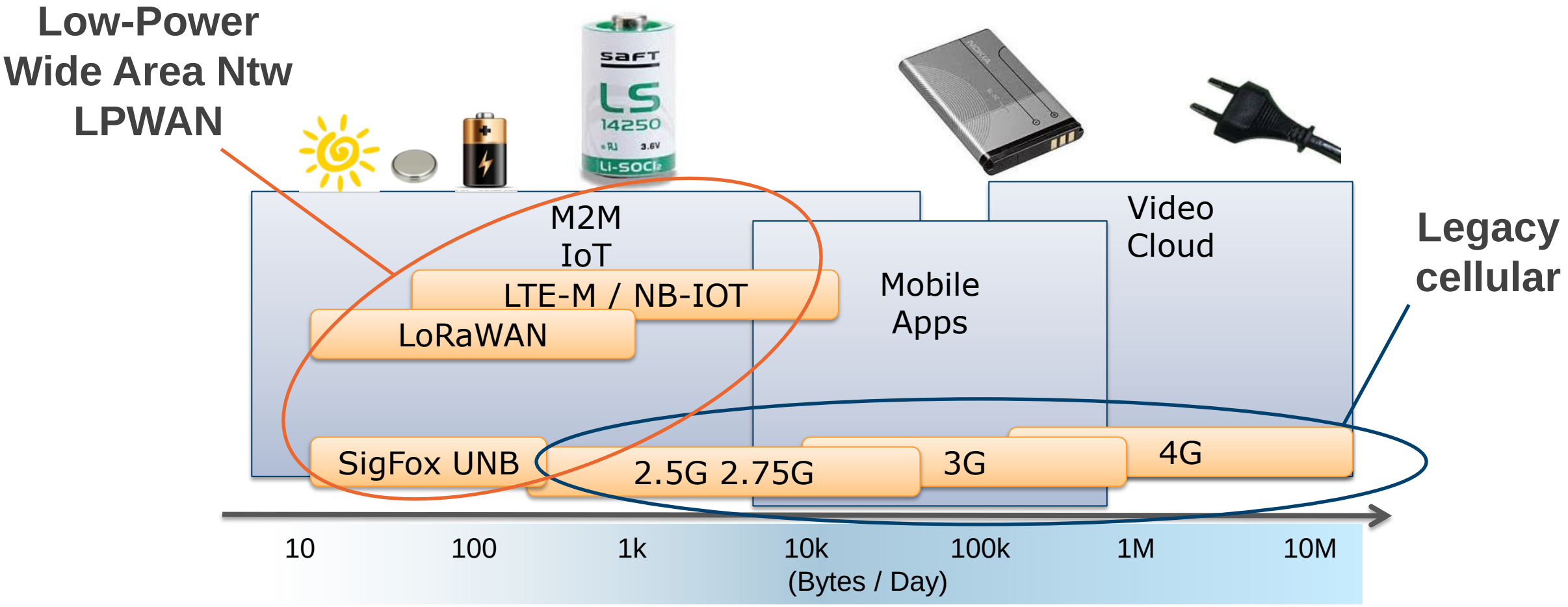
Wireless but no gateway / smartphone



AVNET Memec

SILICA An Avnet Company

Wireless Wide Area Networks – WAN

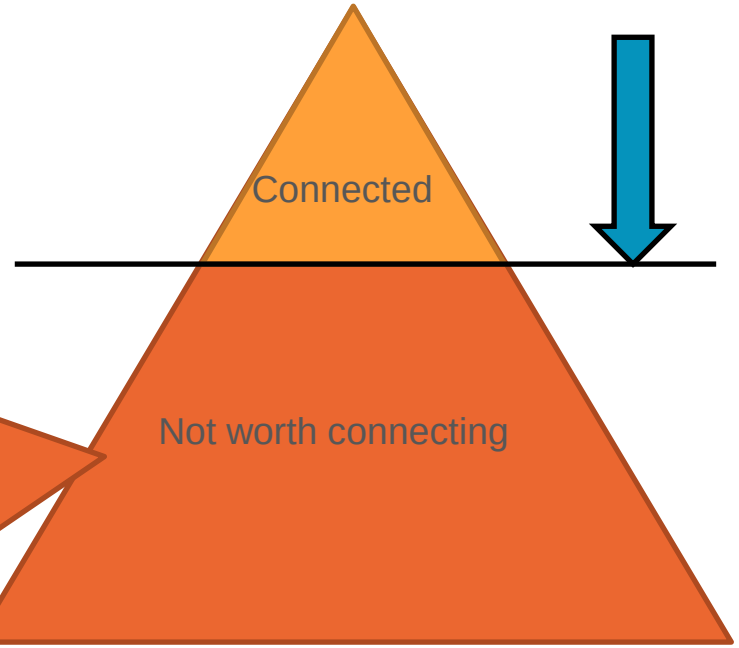


Legacy cellular 2G 3G 4G

- PRO:
  - Operated by MNOs MVNOs since 20 years
  - Massive infrastructure & continued investments
  - Licenced spectrum
  - Ubiquitous service worldwide
  - Secure communication (SIM card)
  - Regulatory body = 3GPP – GSMA
  - Extensive service offering
- Aiming at serving smartphones voice + data
- Aiming at increasing bandwidth 2G → 3G → 4G to fight price erosion
- Legacy M2M communication channel
- CON:
  - not suitable for low-cost battery-operated devices

LPWAN for battery operated devices

Container geolocation tag
Connected HVAC systems
Connected call buttons
Animal Tracking
Bicycle antitheft and geolocation
Industrial logistics
Consumer accessories
…
+ >200 new ideas



…75% of the M2M market by 2020!

LPWAN for battery operated devices

- 2012: SIGFOX invented LPWAN with the deployment of their UNB (Ultra-Narrow-Band) network in FR
- 2012: SEMTECH acquires CYCLEO a French start-up inventor of the LoRa technology
- 2014: Inception of the LoRa Alliance as an answer to SIGFOX who declined using the LoRa technology for their network
- 2015: 3GPP and GSMA have started working together on a NB-IoT standard aiming at providing improved service in licenced spectrum in the frame of a 4G upgrade
  - LoRaWAN & SIGFOX not retained
  - Objective is to deliver a standard by end of 2015

LoRa Technology

Why are LPWANs “long-range” ?

- A longer listening time per bit helps bring the noise level down

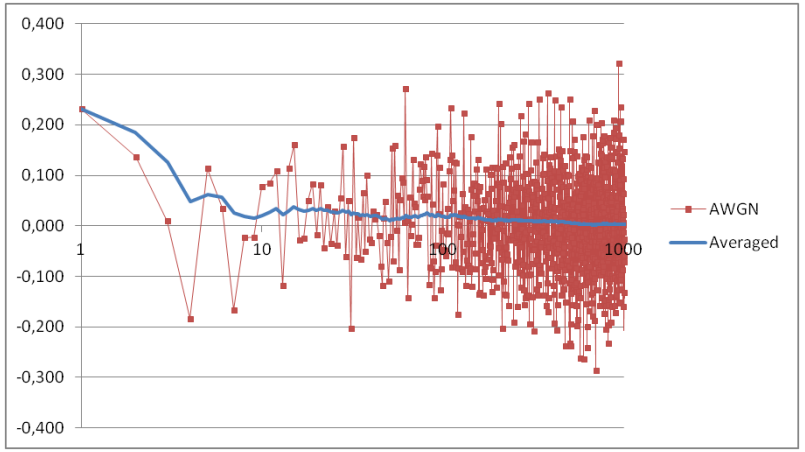
- Bit duration x2
  - Energy per bit x2 (+6dB)
  - Noise energy x sqrt(2) (+3dB)

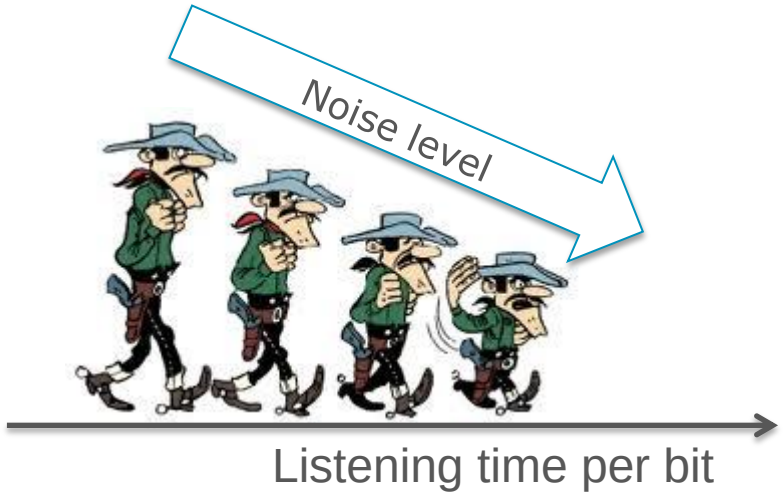
  → Improvement of SNR by 3dB

- From 2G to LoRa
  - 200kbps → 100bps
  - Bit duration extended by factor x2000
  - Range improvement x sqrt(2000) = x45 in open space at iso Tx power

  → Wider cells, less capex for operator

  → Same for Sigfox





LoRa Radio Characteristics

Spread Spectrum – LoRaWAN

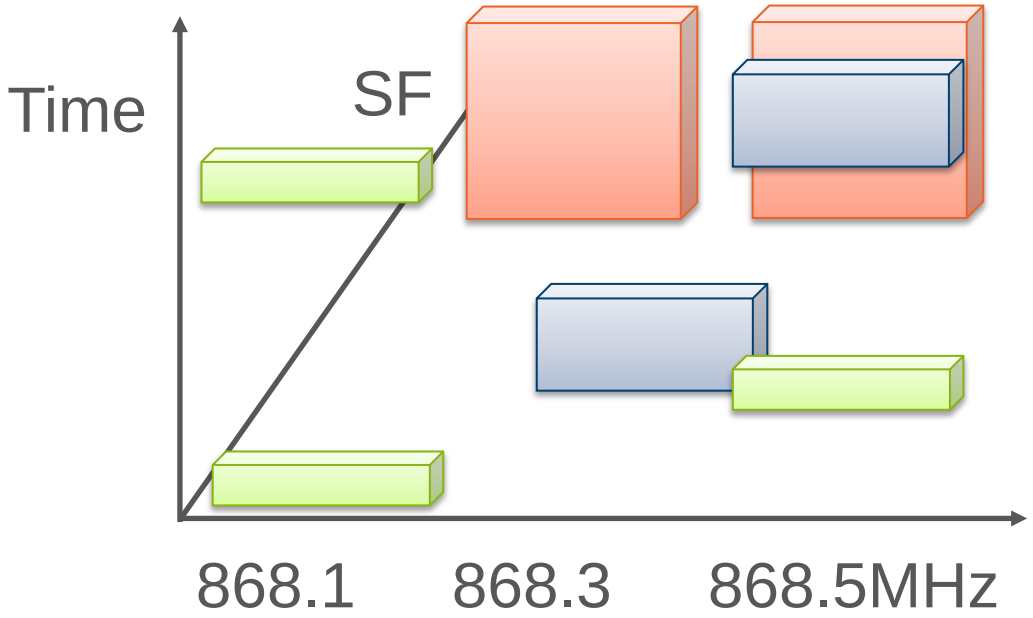
- Uplink:
  - LoRa 0.3-50 kbits per second (Adaptive Data Rate)
  - Link budget = +14dBm (Tx) – -140dBm (ntw sensitivity) = 154dB >> GPRS
  - 10-50 bytes/message payload
  - Message duration = 40ms – 1.2s
  - Energy spent per message Etx = 1.2s x 50mA = 17µAh at full sensitivity
  - Energy spent per message Etx = 40ms x 50mA = 0.6µAh at min sensitivity

- Downlink:
  - LoRa 0.3-50 kbits per second
  - Link budget = +27dBm (Tx) – -135dBm (node sensitivity) = 162dB >> GPRS
  - Message duration = 40ms – 1.2s with average latency of 2s
  - Energy spent per message Erx = 3s x 11mA = 9µAh at full sensitivity

LoRaWAN Spectrum Access

Spread Spectrum – LoRaWAN

- 3 frequency channels 125kHz each
- 6 Spreading Factors (SF) orthogonal between them yielding bitrates from 300bps-50kbps
- Base-station capacity = 3 x 24 x 3600 x 10% = 26k mess/day @ max link budget (SF12)
- Base-station capacity = 3 x 32 x 24 x 3600 x 10% = 829k mess/day @ min link budget (SF7) (= max - 15dB)



LoRaWAN Classes

LoRaWAN

- Class-A
  - Uplink initiated by Node based on Node's need.
  - Class A operation gives the lowest power Device.
- Class-B
  - Sensors are synchronized by network beaconing - TDMA
  - Unlikely in public deployment
  - Useful in private networks for throughput optimization
- Class-C
  - Mains-powered sensors/actuators can be in listen-mode full-time

LoRaWAN Standard

The LoRa™ Alliance (http://lora-alliance.org/) is an open, nonprofit association of members.

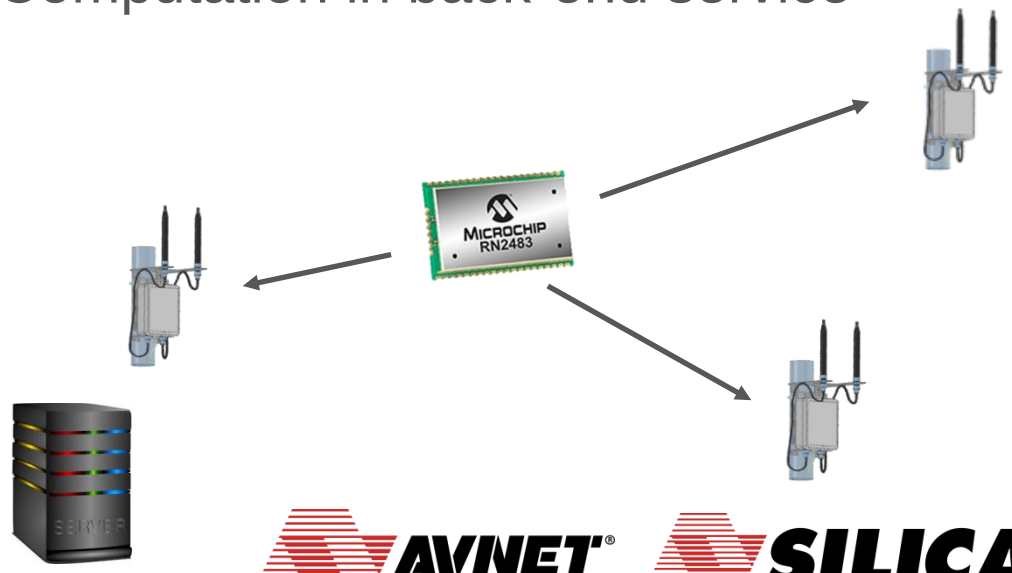
Mission: to standardize Low Power Wide Area Networks (LPWAN)

Alliance members will collaborate to drive the global success of the LoRaWAN™ protocol

What LoRa can do that others cannot

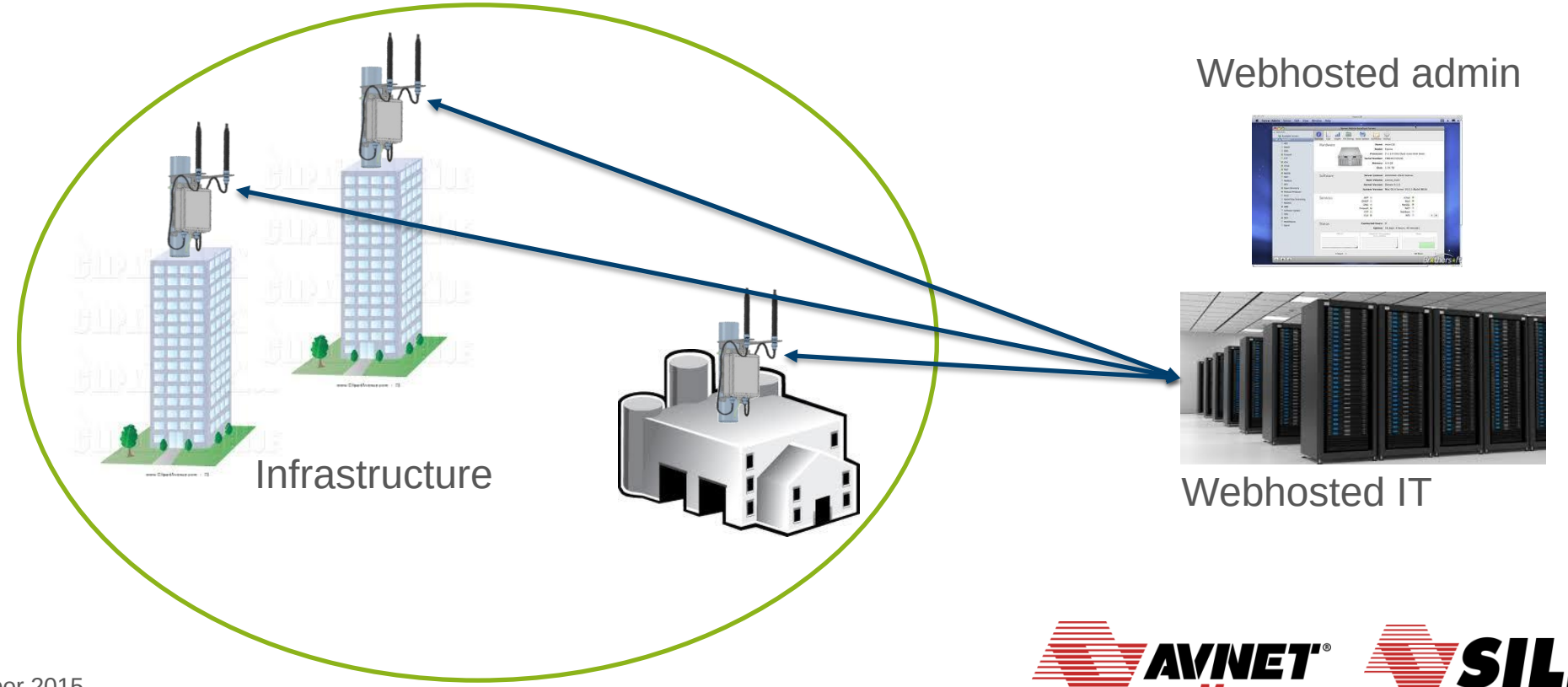
- Geolocation without GPS
- Even works indoor!
- … provided that the node is seen by at least 3 base-station
- Heavily depends on the operator deployment strategy
- Operational in Q2 2016
- Supported in latest revision of gateway hardware and stack

- How does it work ? DTOA: Differential Time of Arrival
- If base-stations are time synchronized and can time-stamp received messages with a precision of 100ns = 30m
- Computation in back-end service



LoraWAN Private network infrastructure

- Customer owns, installs and administrates his private network across his buildings and campuses
- Connects sensors, actuators, machines inside Intranet
- Compatible with public networks when available
- Also useful to strengthen / complement a public network in harsh industrial environments



Where can we use this?

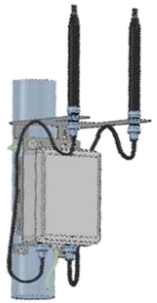








LoRa Available Hardware / Software

Gateways : 

Kerlink, Actility…

Modules : 

Microchip, Telecom Design……

Tranceivers : 

Semtech SX127x series

Developement Tools : 

Software stack for Nodes :
https://github.com/Lora-net/LoRaMac-node

Base Station/ Server Software : Actility, IBM..

AVNET Memec SILICA An Avnet Company

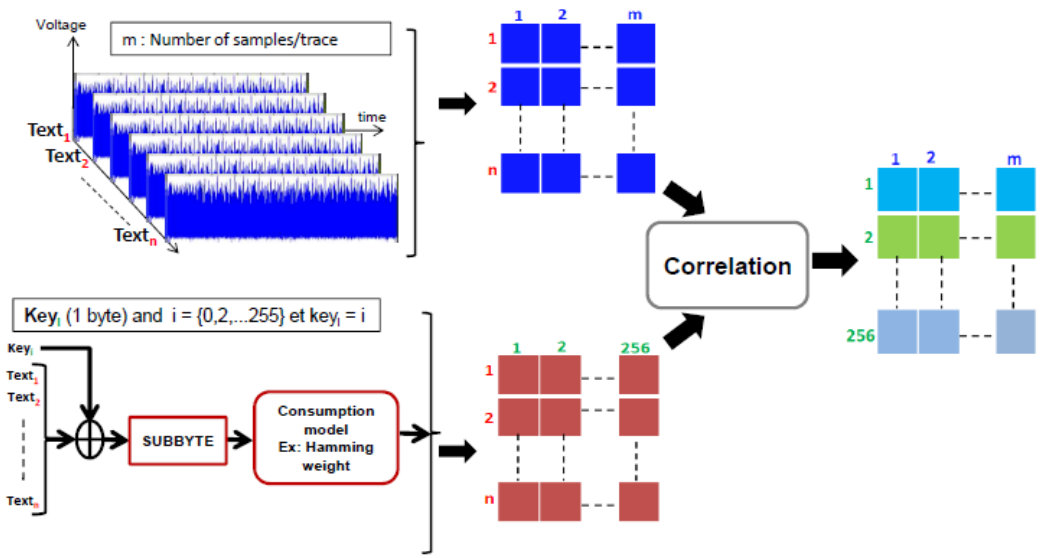
IoT Security

Being connected is great unless…

… you get exposed while poorly protected

How secure is security?

It takes 16min, a laptop, Matlab, a 150€ USB oscilloscope & probe to extract an AES128 key from any non-secure MCU



Courtesy of Driss Aboulkassimi – CEATech – FR – driss.aboulkassimi@cea.fr

State-of-the-art CRYPTOGRAPHY in History
Contemporary period

Franck Miller
One-Time-Pad –
Polyalphabetic
substitution
“Perfect secrecy”

Radio

Alan Turing
Claude Shannon
Modern
cryptography

Diffie-Hellman
invention of
public key

RSA
Rivest, Shamir,
Adleman

www

Wireless
www
& IoT

AES
WEP
SSH
WPA
WPA2
PGP
Cheap Secure
Element

1880 1900 1920 1945 1975 1990 2000 2010

Sir William
Herschel -
fingerprints

First
transatlantic
radio
transmission

ENIGMA

UWB
CDMA
DES

EMVco
Banking
smart card
SIM card
ECC
Koblitz, Miller

SHA-
SSL
TLS

IPv6
802.15.4
iPhone

SHA-2
SHA-3
LWC

perfect secrecy

- Does perfect secrecy exist ?

→ YES with the one-time pad – inconvenient: length(key) >= length(message)

- Can we have perfect secrecy with length(key) < length(message) ?

→ NO

- Is it a problem, ie is perfect secrecy what we need ?

→ NO – we need “good enough” secrecy:

- length(key) << length(message)
- can only be broken with probability << ε
- can only be broken with unrealistic computation complexity

- Does such secrecy exist ?

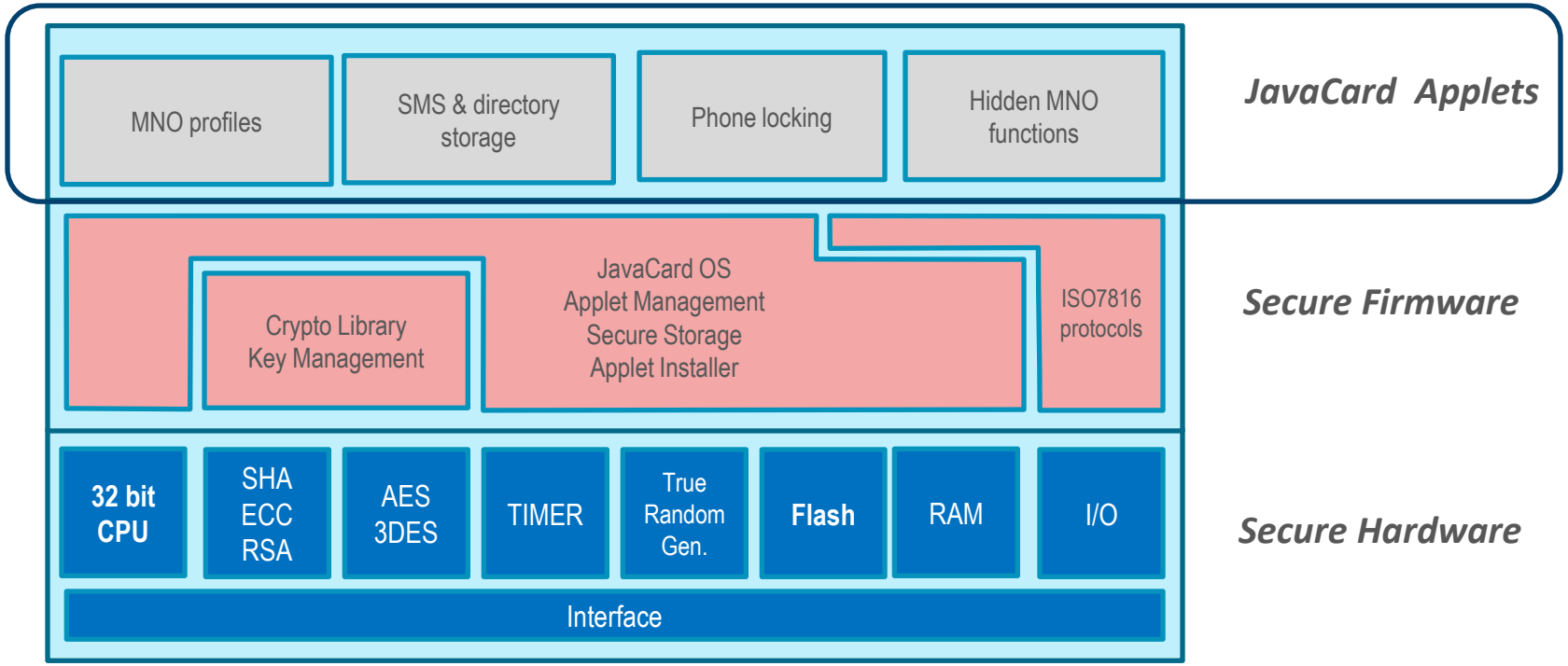
→ YES – RSA / AES / SHA / ECC can provide this level of performance

Cryptography is mature

- Since RSA, AES, ECC, SHA, cryptography has reached maturity
- “Cryptography is now by far the best settled part of Information Security” (Whitfield Diffie, 2005)
- Computational complexity for brute-force attack ~ 2^length(key)
  - 2048-bit key takes 2^2048 ~ 10^600 steps to solve
  - 10^82 atoms in universe
  - Assuming // computing with 1 computer per atom still takes > 10^500 steps per computer
  - Assuming lightning-fast computing with 10^100 steps per second
  - Computation would take 10^400 seconds >> life-time of galaxy

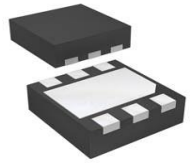
What is a UICC / SIM card ?

Customized and personalized by the MNO/VNO for the subscriber

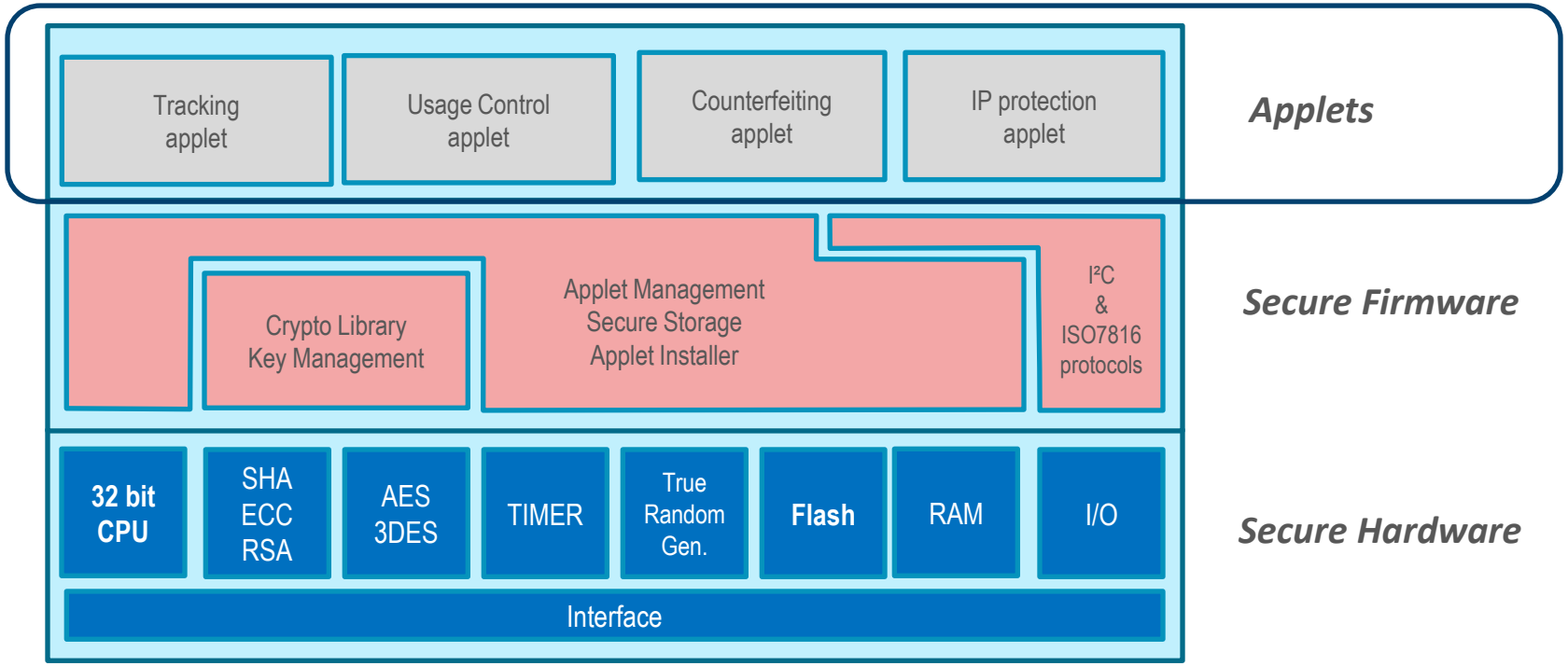


What is a secure element ?

TRUSTED OBJECTS



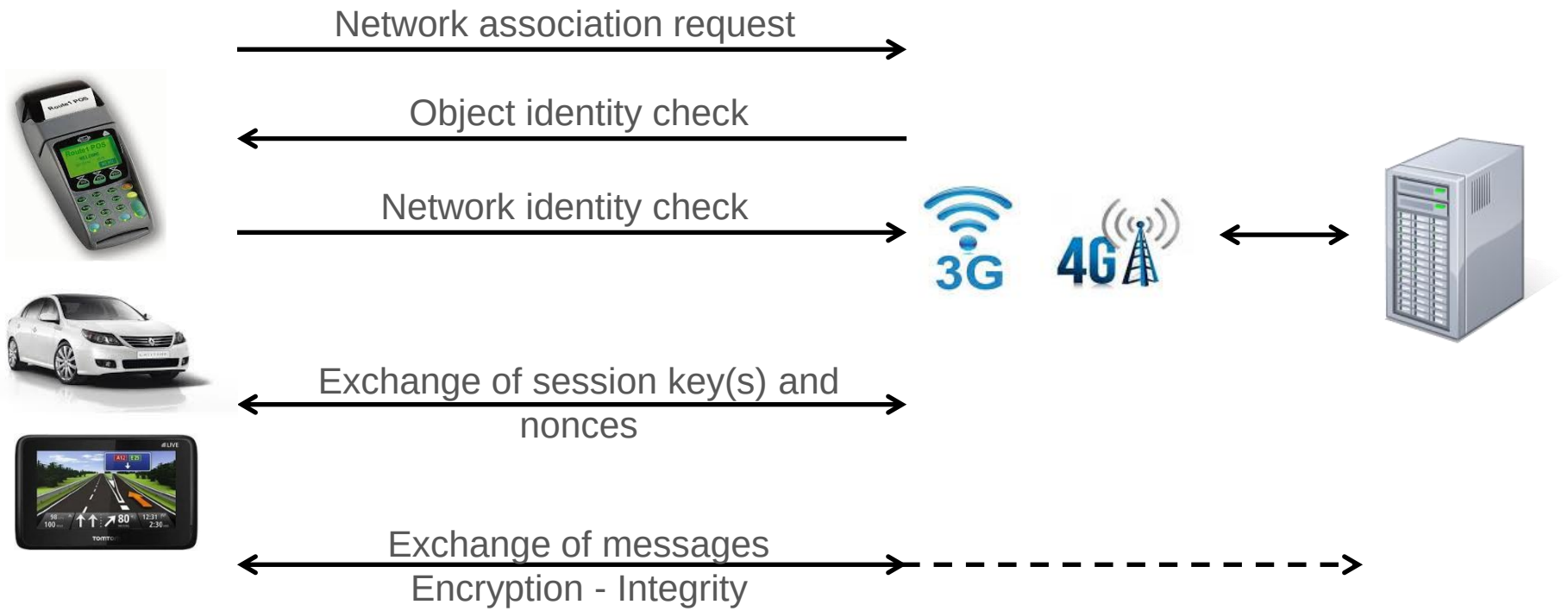
Customized and personalized by AVNET for the client



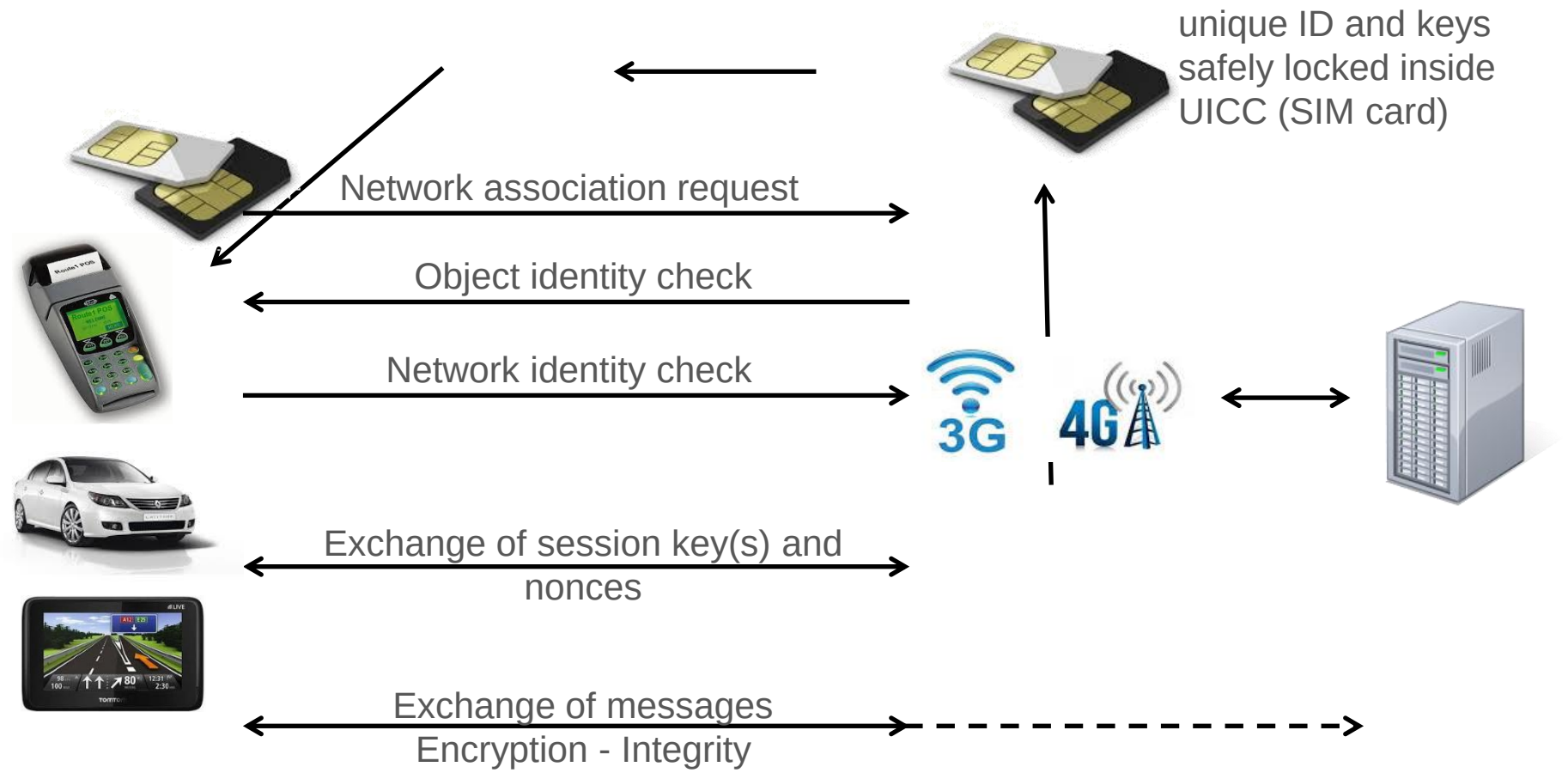
AVNET Memec

SILICA An Avnet Company

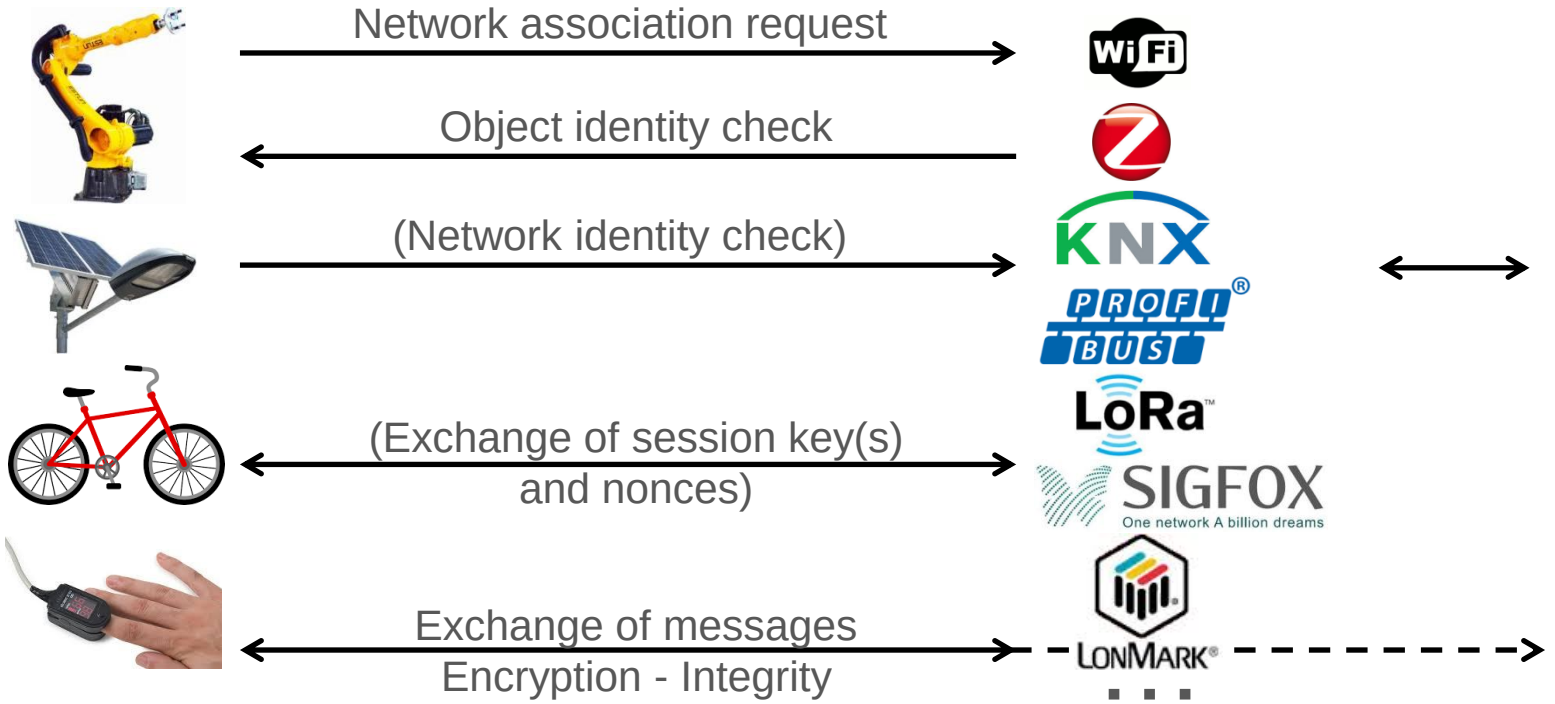
2G/3G/4G - connectivity protocol (simplified)



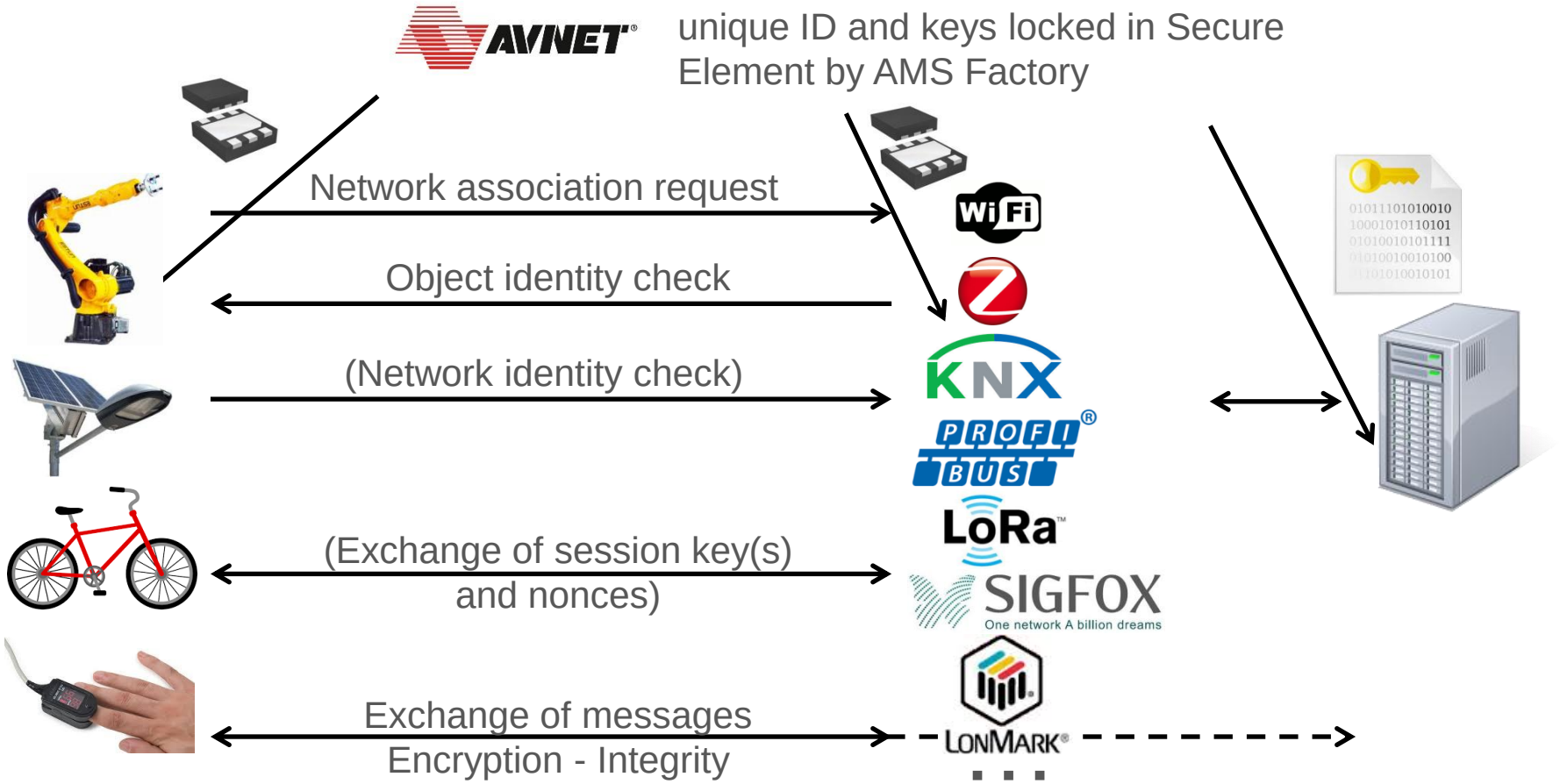
2G/3G/4G - HW security handled by SIM card



Other LAN and WAN - same connectivity protocol model



Other LAN and WAN - HW Security handled by secure element



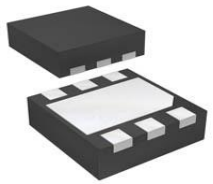
AVNET Memec
SILICA An Avnet Company

AMS 100% secure supply chain

TRUSTED OBJECTS

Supply chain is EMV Co compliant

AVNET Logistics



Secure boot-loader

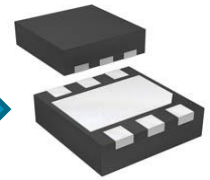
Chip is « unlocked »

Firmware & Applet are loaded

Chip is personalized with secret keys
Every chip is unique

Secure logistics

Customer



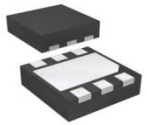
User keys and certificates are generated by Avnet's secure servers

AVNET Memec

SILICA An Avnet Company

Beyond wireless - applications of a Secure Element

TRUSTED OBJECTS



Authentication of removable part, consumable, electronic board….

Protection against unauthorized modifications of software

Integrity control of every node of a network

Sensitive data secure storage

Usage control of peripherals (medical)

Secure login to remote system

Anti-Cloning

Secure tracking

IP protection

Usage control

AVNET Memec

SILICA An Avnet Company


Thank you.