Open EUREKA INNOVATION WEEK BARCELONA 15-19 MAY 2017
Sharing technology

gemalto security to be free

Building a *trusted* Internet of Things: Secure, Connect, Monetize

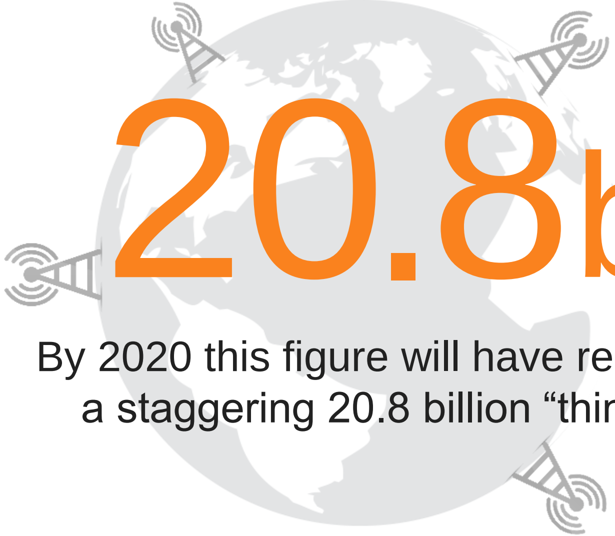
Jean-Pierre Tual, Gemalto, VP Open Innovation Barcelona, May 19th, 2017

The Connected World

The “things” on our planet are connecting far faster than we can imagine.

6.4b

“things” connected
around the globe in 2016



20.8b

By 2020 this figure will have reached
a staggering 20.8 billion “things”

In our daily lives we will depend on the knowledge flowing continuously from the data created by these billions of connected “things”

Source: Gartner 2015

IoT transforms a variety of markets

The industrial IoT market is set for major growth and expected to reach $151 billion by 2020(1)
Many sectors will benefit from industrial IoT including:

Fleet Management – global fleet management market is estimated to grow from $8.03 Billion in 2015 to **$22.35 Billion by 2020**, driven by new technology and IoT (2)

close to **35 million connected POS** (3) terminals in use around the world in 2015

Connected Cars – **380 million connected** cars on the road by 2021(4)

1.8 billion connected home units (5) shipped in 2019 including Physical Security / Home alarms

Energy – almost **800 million** electric smart meters to be installed globally by 2020(6)

mHealth – the M2M healthcare industry will generate **USD90.9 billion** in total revenues by 2023(7)

Source: (1) MarketsandMarkets (2) MarketsandMarkets (3)Nilson BI Intelligence (4) BI Intelligence (5) Business Insider, (6) Telefonica (7) Machina Research

IoT and the Connected Person

IoT will connect us through every moment of our daily routines – from our **smart homes** to our **cars** to our **offices**, to **personal health** and **fitness** and beyond.

By **2022**, the average household with two teenage children will own approximately **50 Internet connected devices**.

Source: Organization for Economic Co-Operation & Development

Total value of IoT services will hit

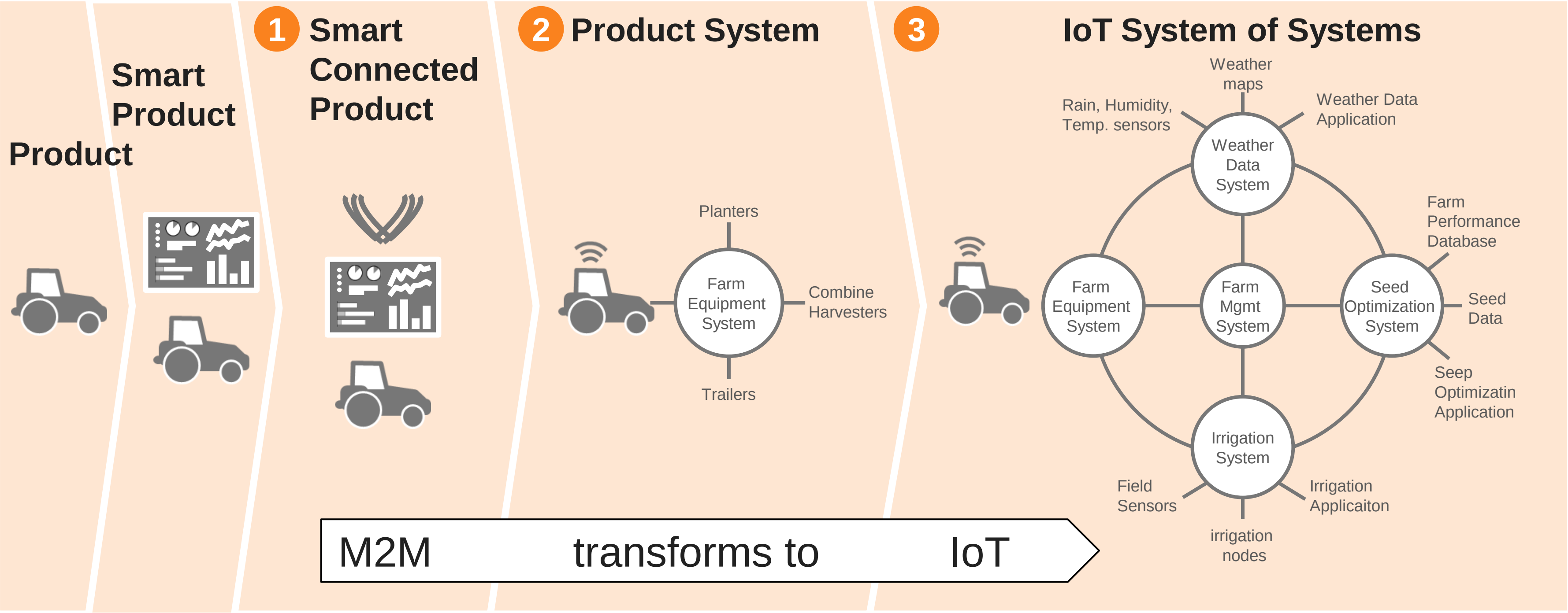
$290 billion

by 2020, more than doubling

from $138 billion in 2015.

Source: Juniper Research

M2M goes IoT – a phase of business transformation



Product

Smart Product

1 Smart Connected Product

2 Product System

Planters

Farm Equipment System

Combine Harvesters

Trailers

3 IoT System of Systems

Weather maps

Rain, Humidity, Temp. sensors

Weather Data Application

Weather Data System

Farm Performance Database

Farm Equipment System

Farm Mgmt System

Seed Optimization System

Seed Data

Seep Optimizatin Application

Irrigation System

Field Sensors

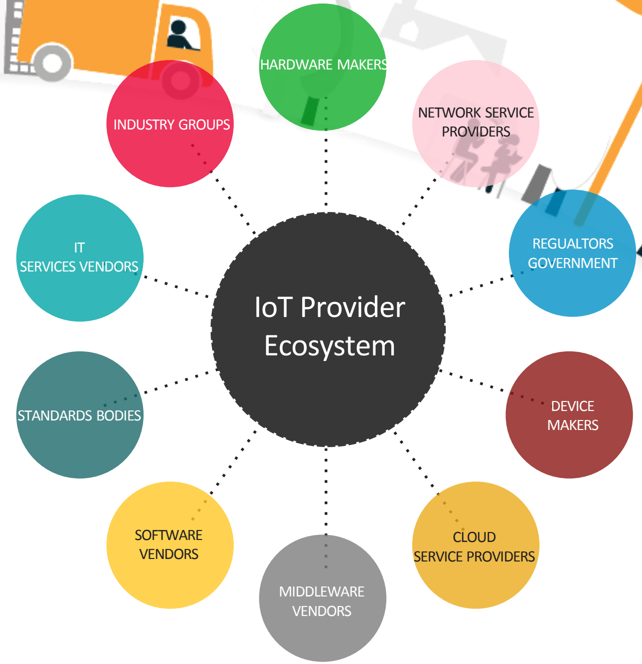
Irrigation Applicaiton

irrigation nodes

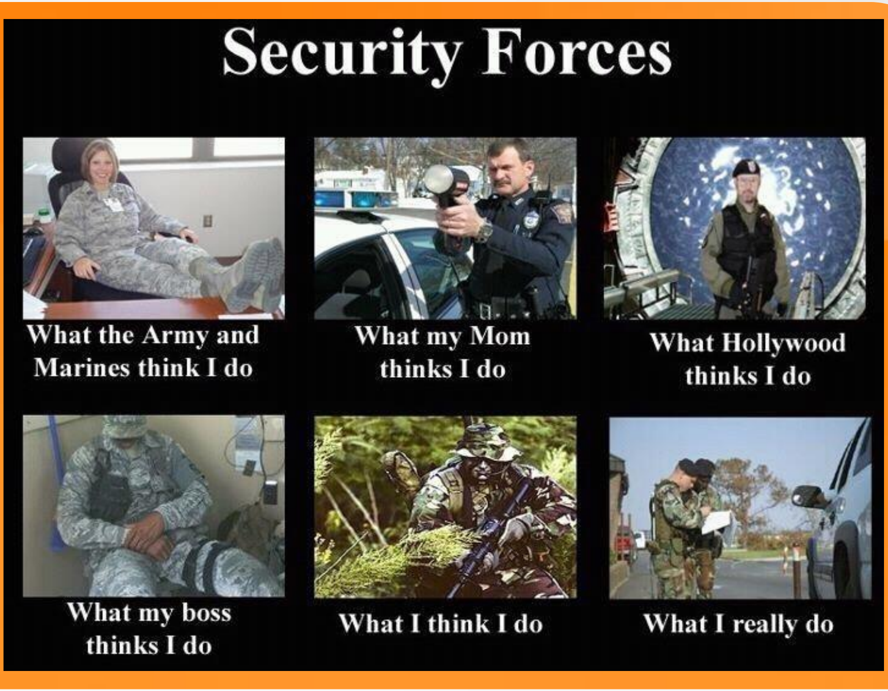
M2M transforms to IoT

The Foundation of Trust in IoT

- A reliable **security** framework
- A reliable **Connectivity** framework
- An agile **monetization** framework

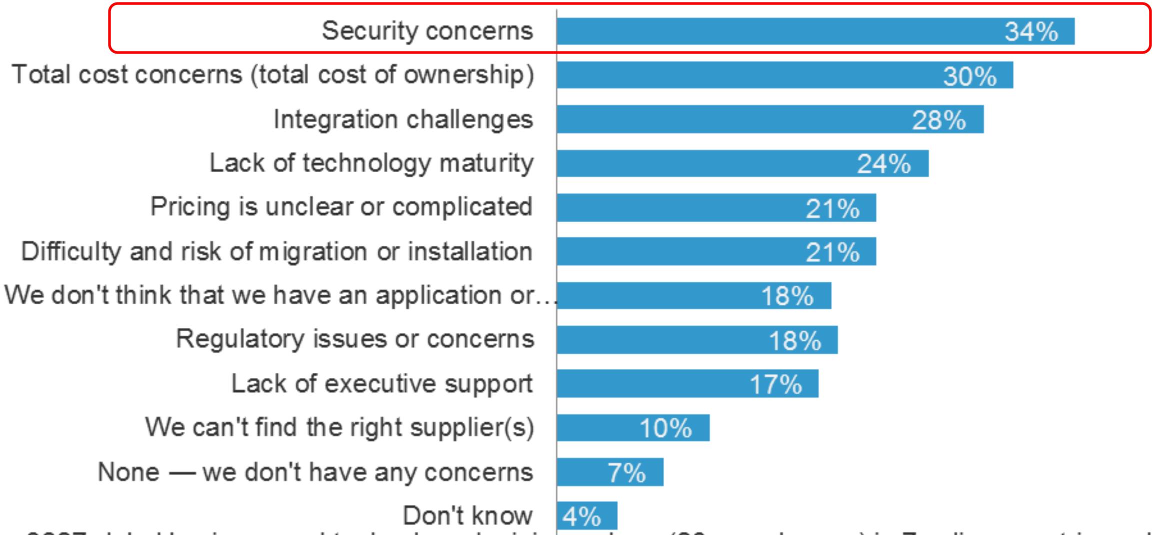


SECURE


Security Forces
What the Army and Marines think I do
What my Mom thinks I do
What Hollywood thinks I do
What my boss thinks I do
What I think I do
What I really do

But Security tops the list of IoT concerns

What are your firm’s concerns, if any, with deploying M2M/Internet of Things technologies? *(All that apply)*



Base: 3627 global business and technology decision makers (20+ employees) in 7 online countries only

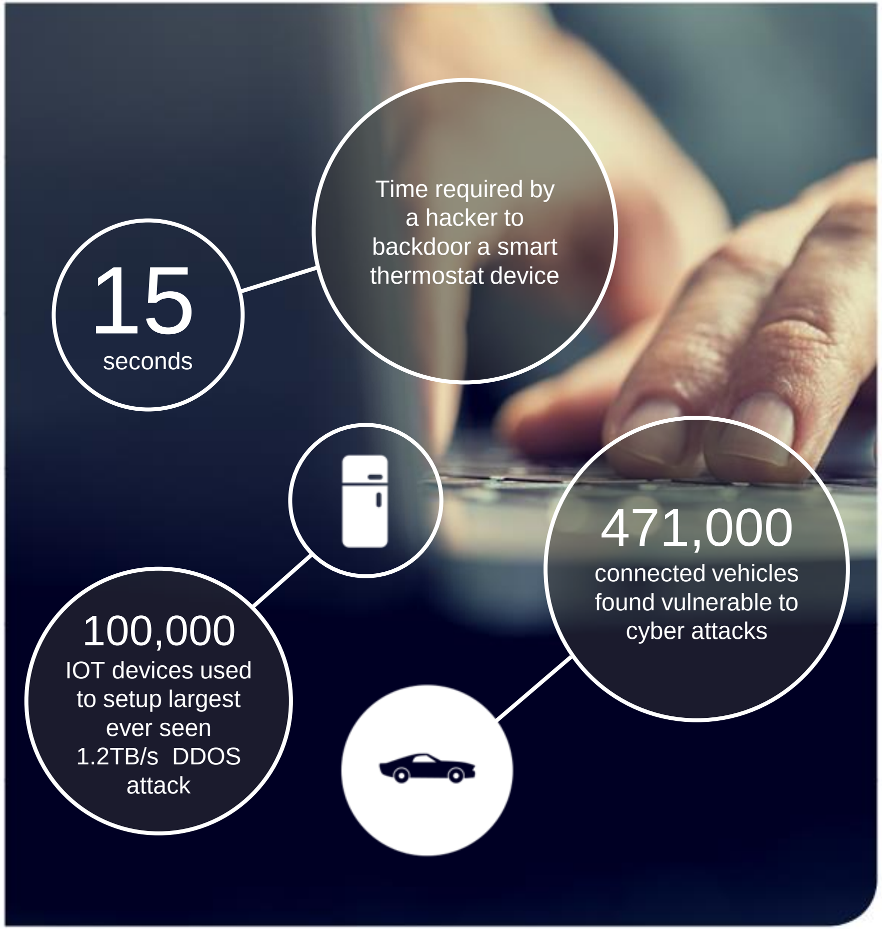
Source: Forrester’s Global Business Technographics® Networks And Telecommunications Survey, 2015

Authentication, data protection and Privacy is Critical

- Consumers and Enterprises only want authorized entities to have access to their devices or data

- Secure components and solutions must be embedded into “things” to protect data

- Hackers will take advantage, whenever there is a security loophole



15 seconds

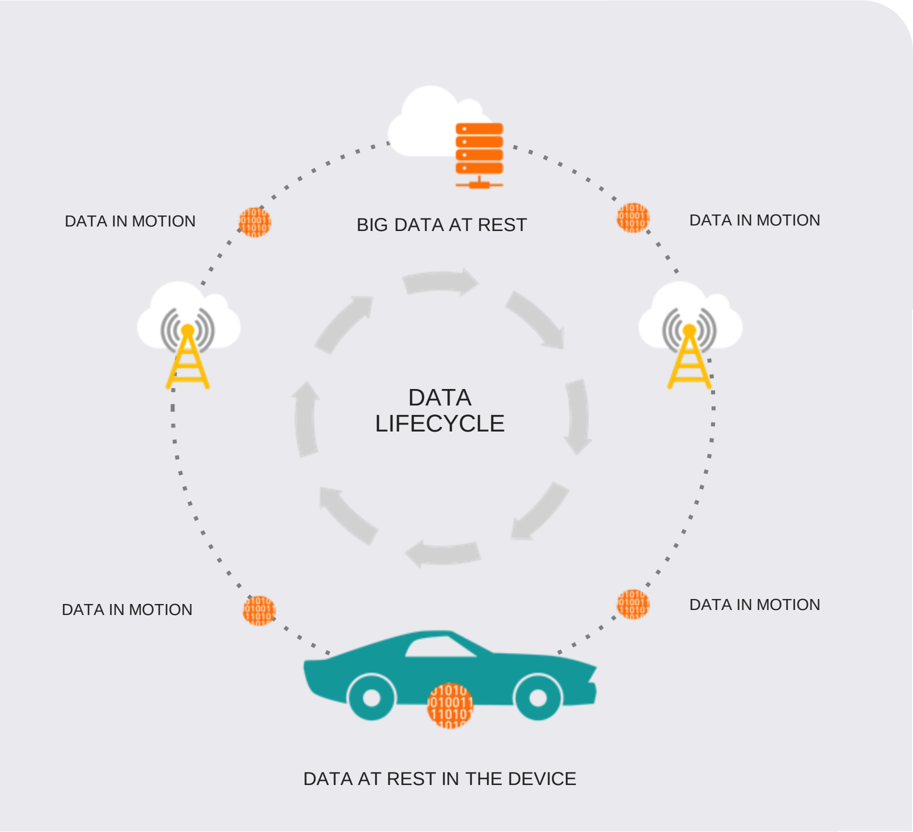
Time required by a hacker to backdoor a smart thermostat device

471,000 connected vehicles found vulnerable to cyber attacks

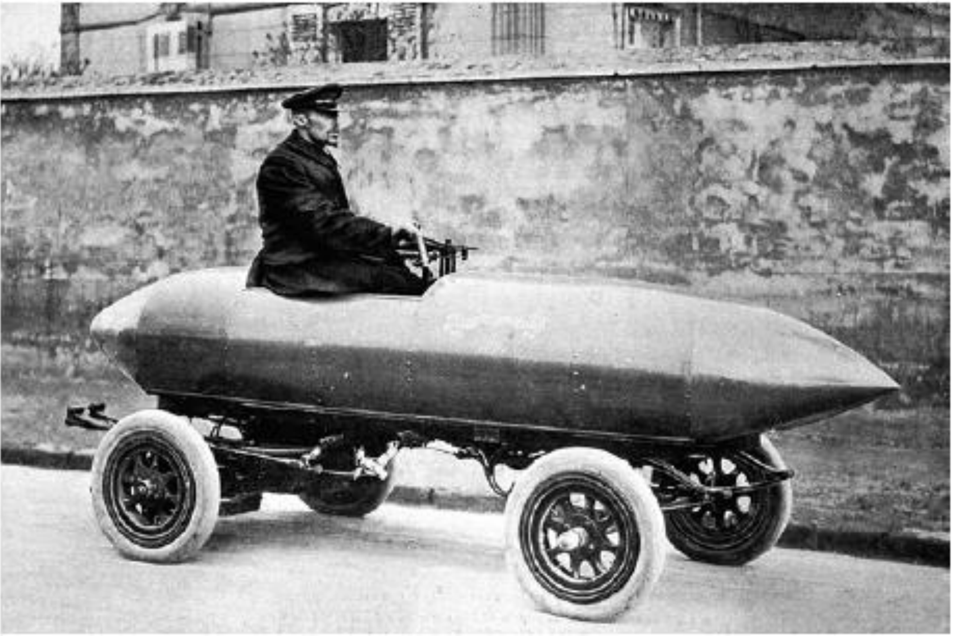
100,000 IOT devices used to setup largest ever seen 1.2TB/s DDOS attack

Influx of Data in Connected Ecosystems

- Data is ***at rest*** in the device and in the cloud
- Or ***in motion*** between devices and the cloud
- The nature of data varies, such as vehicle location data or streamed media
- Which requires different levels of privacy and security



Example: electric vehicles

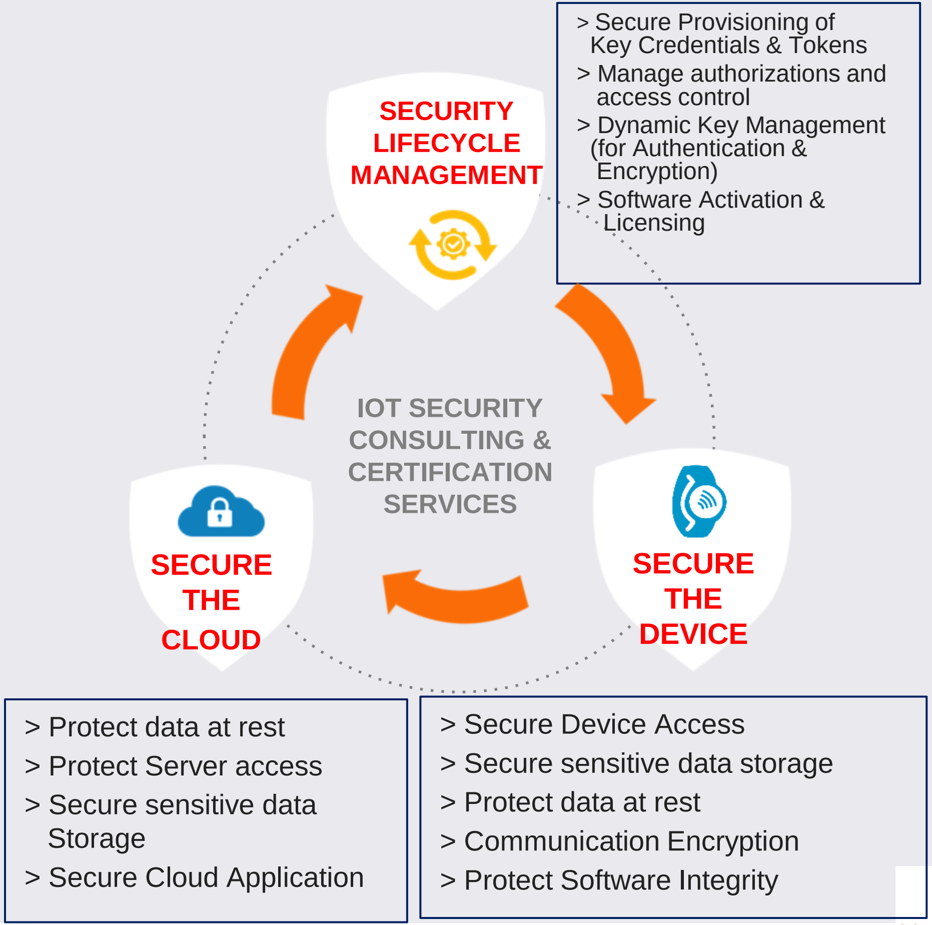


0 B of data uploaded over life-time

~25 GB of data uploaded every hour

Secure

Practical approach to security closes the loop, managing the complete security lifecycle of the connected objects together with data at rest and in motion from the network to the cloud.



SECURITY LIFECYCLE MANAGEMENT

- > Secure Provisioning of Key Credentials & Tokens
- > Manage authorizations and access control
- > Dynamic Key Management (for Authentication & Encryption)
- > Software Activation & Licensing

IOT SECURITY CONSULTING & CERTIFICATION SERVICES

SECURE THE CLOUD

- > Protect data at rest
- > Protect Server access
- > Secure sensitive data Storage
- > Secure Cloud Application

SECURE THE DEVICE

- > Secure Device Access
- > Secure sensitive data storage
- > Protect data at rest
- > Communication Encryption
- > Protect Software Integrity

Method is the key to good security

Building a Secure IoT with e2e Security

Method is the key to good security

1 **Assess** the **security needs** of the infrastructure through a risk evaluation : Security by design

- Identify the security Goals
- Identify the assets to protect
- Identify the threats to those assets
- Characterize the risks associated to each threats
- Identify the threats to counter and the coutermeasures to put in place

2 **Address the threats from the edge to the core**

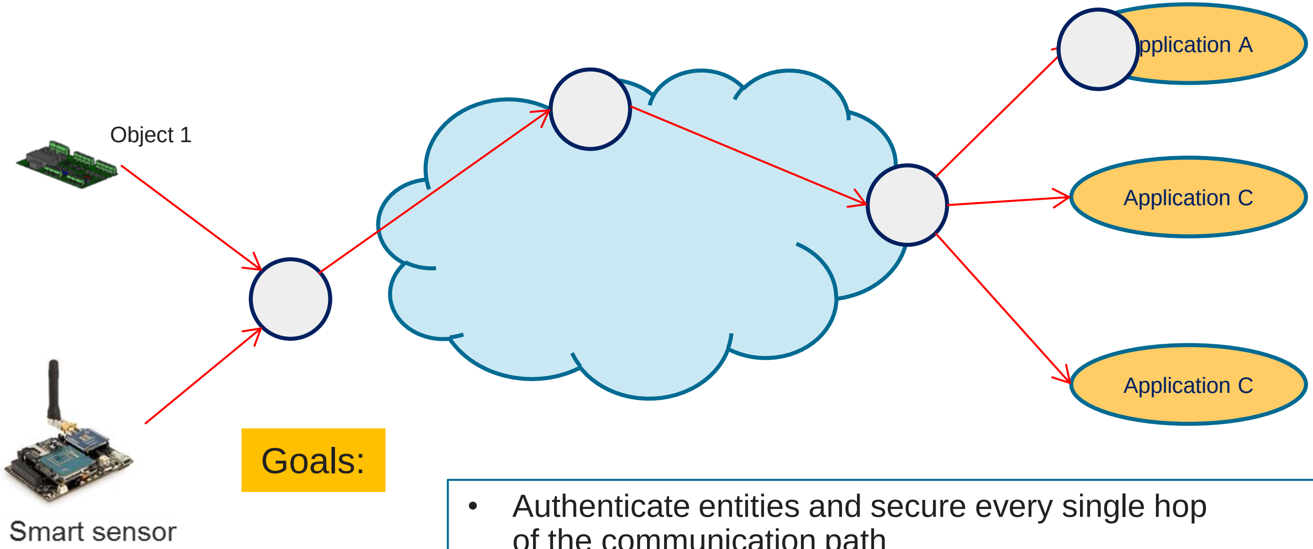
- Each component is uniquely identified
- Encrypt data
- Store and manage keys
- Control user access

3 Make your **security evolve**

- Life cycle management of security credential

IOT security ; heterogeneity is the rule

IOT applications often involve several communication hops between heterogeneous platform nodes



Goals:

- Authenticate entities and secure every single hop of the communication path
- Manage authorizations (fine grain) in every node and control access to protected resources

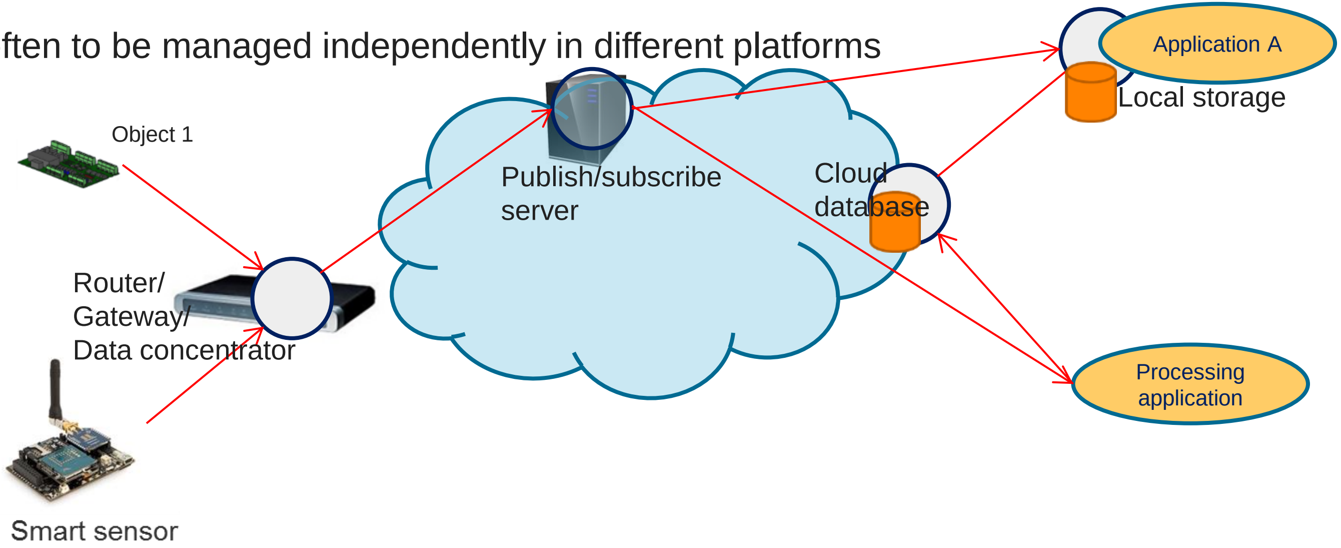
- Credentials have often to be managed independently in many different platforms
- Access control and credential management is cumbersome and error prone

gemalto

IOT heterogeneity illustration

IOT applications often involve several communication hops between heterogeneous platform nodes

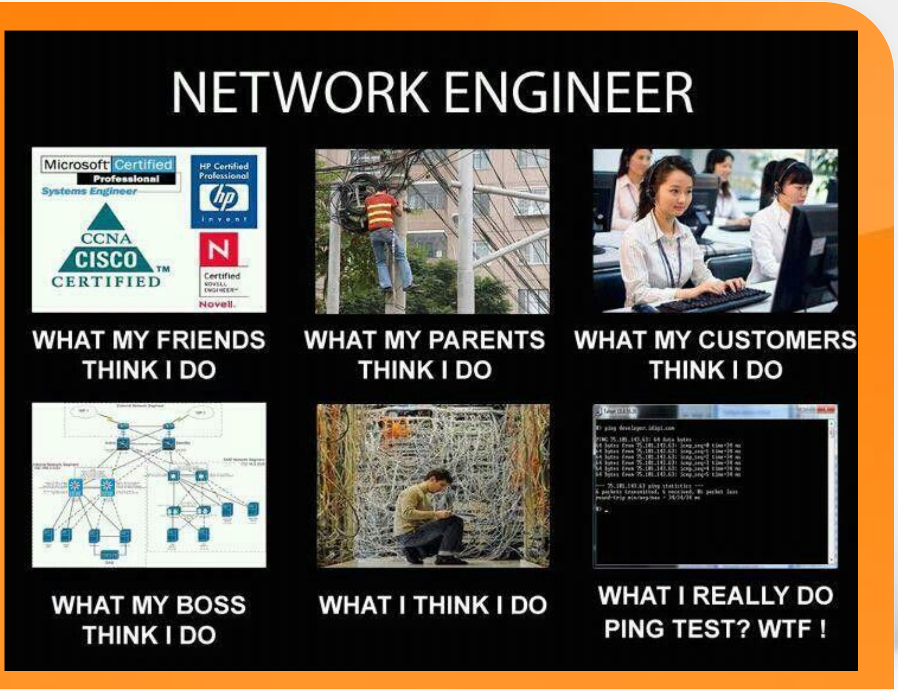
Credentials have often to be managed independently in different platforms



Needs :

- Holistic management of access control and credentials (grant, revoke) in a single place
- Plug and play capability for devices , including security bootstrap

CONNECT


NETWORK ENGINEER
Microsoft Certified Professional Systems Engineer
HP Certified Professional
CCNA CISCO CERTIFIED
Certified NOVELL ENGINEER Novell.
WHAT MY FRIENDS THINK I DO
WHAT MY PARENTS THINK I DO
WHAT MY CUSTOMERS THINK I DO
WHAT MY BOSS THINK I DO
WHAT I THINK I DO
WHAT I REALLY DO PING TEST? WTF !

Context

- Security is like an onion, made of layers
- Setting up application security requires

  network connectivity…..

  which need to be secured

The « connect » mission is to provide instant plug and play network connectivity as devices are deployed in the field.

Then, with this network connectivity more things may happen at deployment time

Connect

Enable
out-of-the box

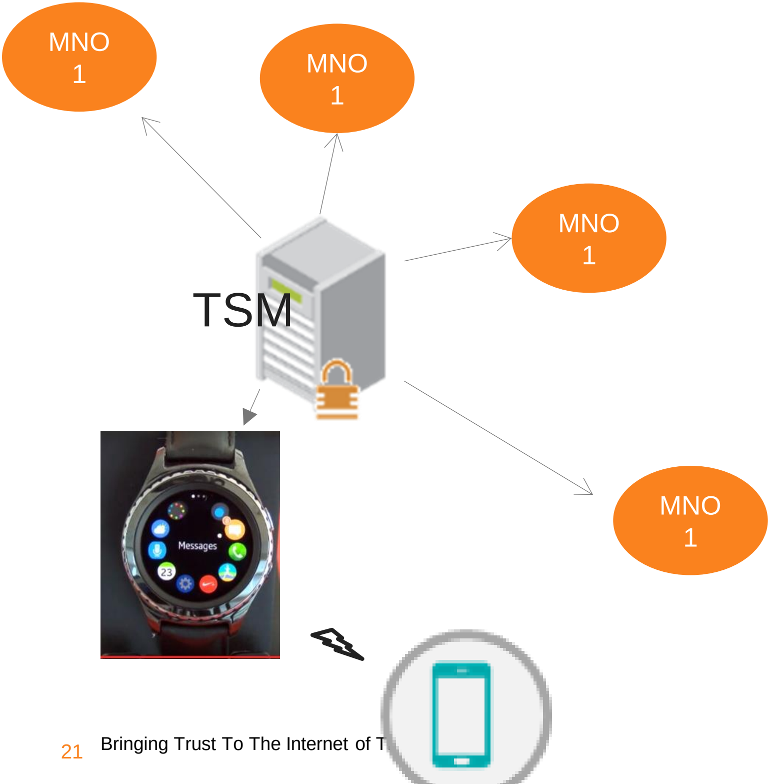
secure connectivity

Flexibility
for diverse device form factors

Ensuring
quality of service

Manage
lifecycle of subscriptions

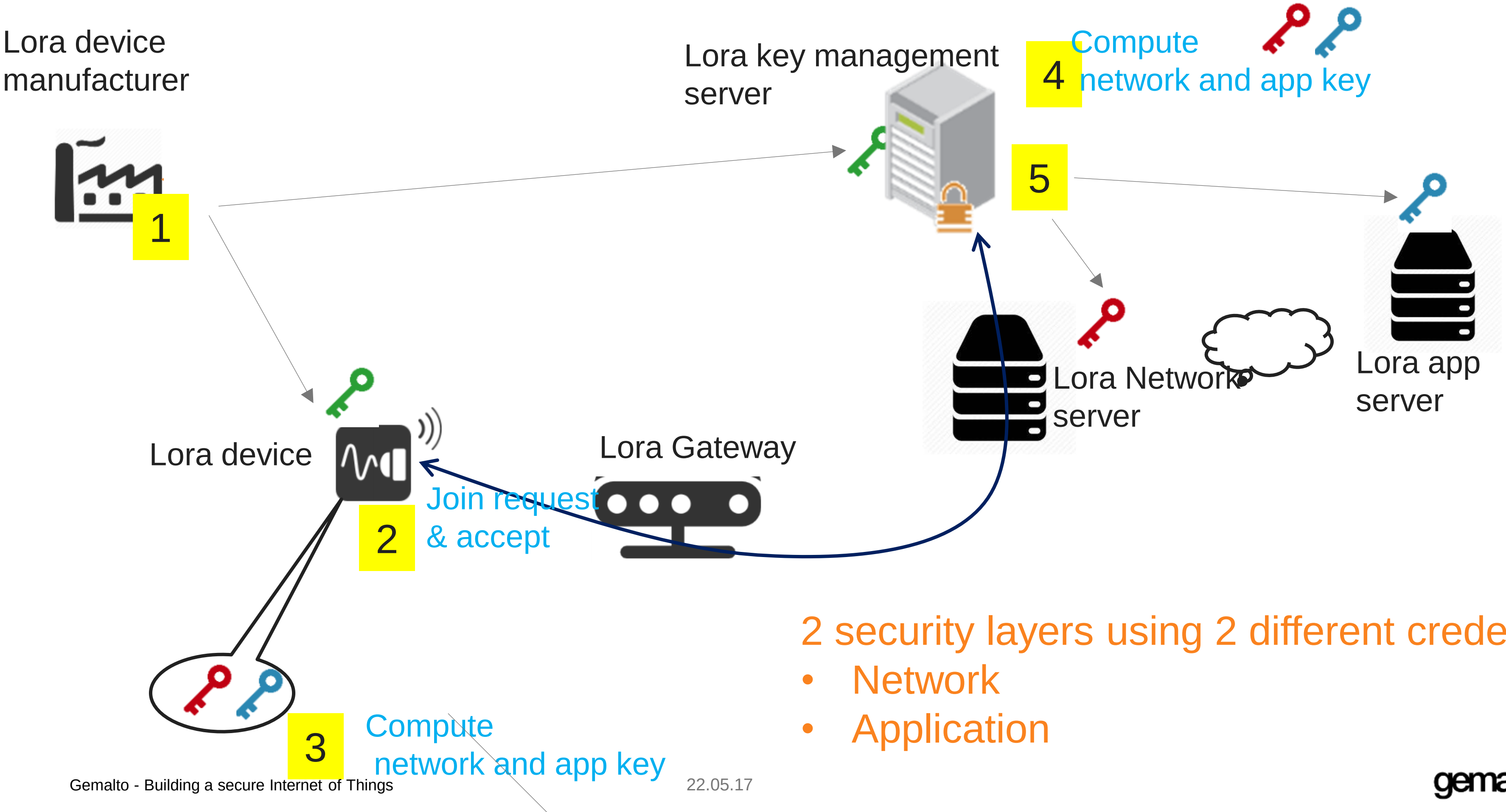
Plug and play secure network connectivity to 3GPP networks



On demand connectivity
smart watch mobile subscription
download:

- User select operator to purchase subscription from
- Subscription is automatically downloaded in the embedded SIM in the smart watch

Lorawan secure plug and play connectivity



Lora device manufacturer

1

Lora key management server

4

Compute network and app key

5

Lora Network server

Lora app server

Lora device

Lora Gateway

2

Join request & accept

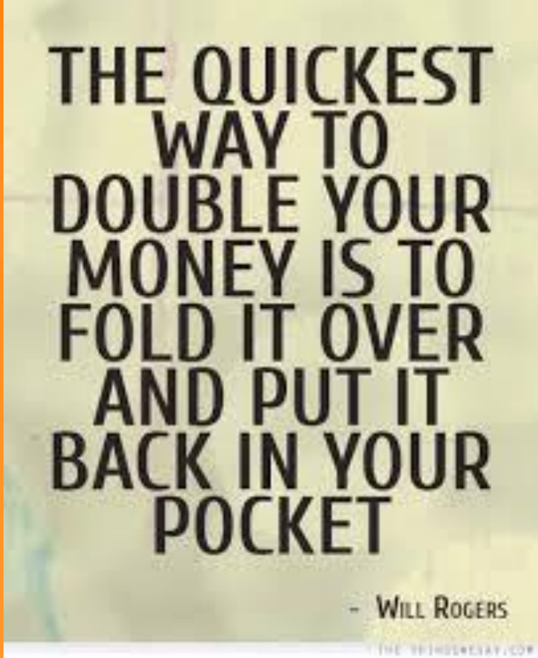
3

Compute network and app key

2 security layers using 2 different credentials

- Network
- Application

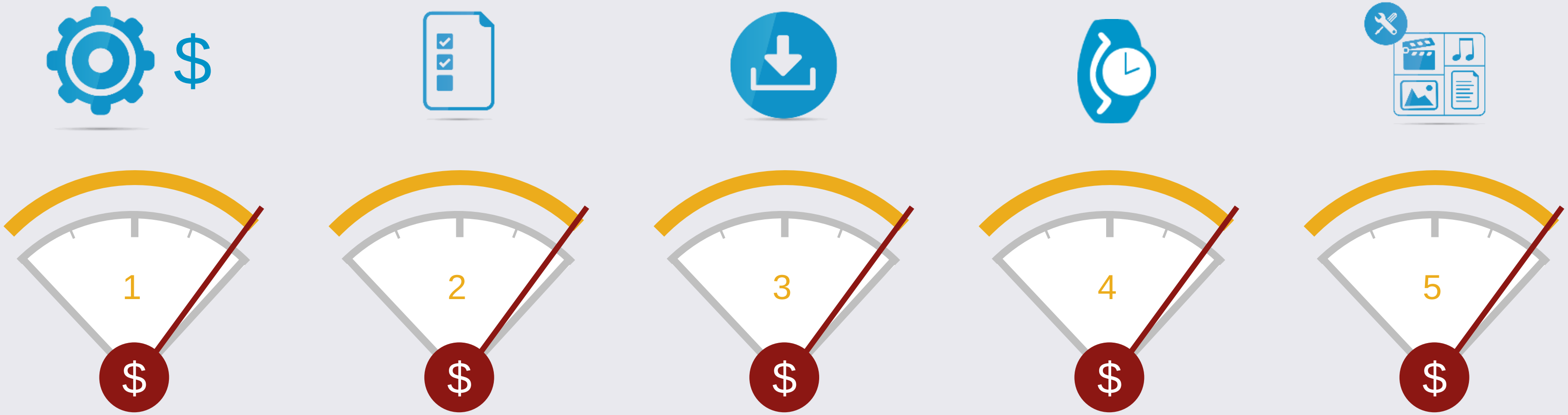
MONETIZE



THE QUICKEST WAY TO DOUBLE YOUR MONEY IS TO FOLD IT OVER AND PUT IT BACK IN YOUR POCKET

- WILL ROGERS

Monetize



1. Enable flexible monetization models
2. License and entitlement management
3. Software upgrades
4. Device management
5. IoT application development

Realizing the Benefits of a Totally Connected World

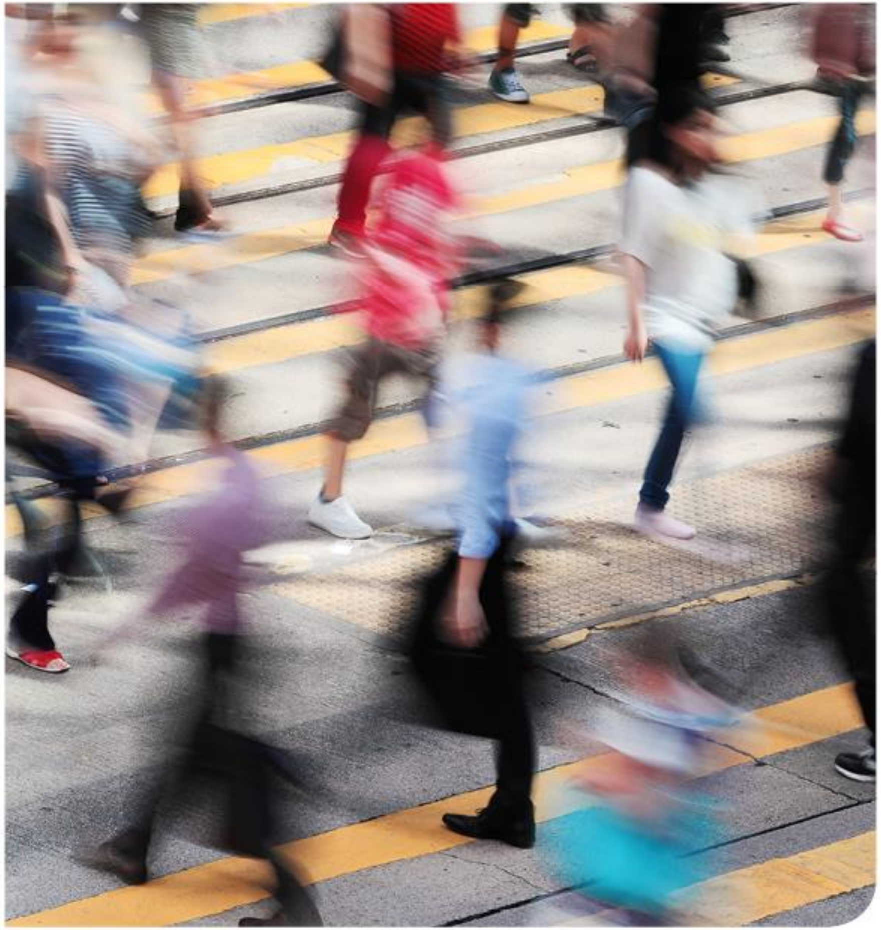
Reduce risks and impacts associated with security breaches

Lower operating costs for business

More opportunity to partner

Business continuity

New business models

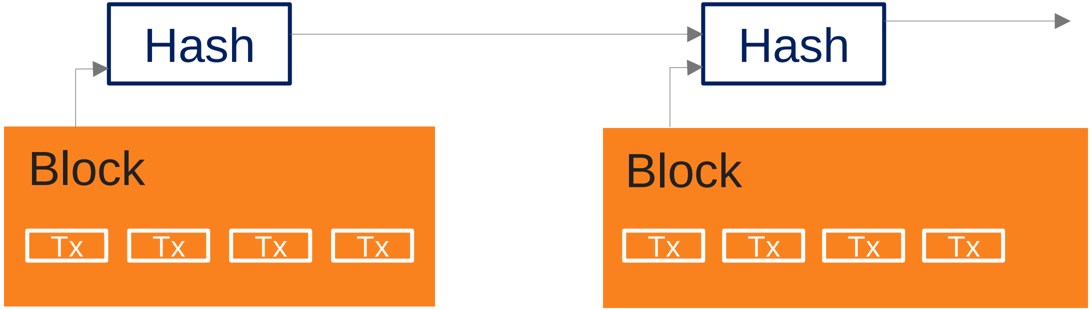


Blockchain: a (potentially) disrupting technology

secure

monetize

- Blockchain: a decentralized secure append-only database
- Used to create distributed ledgers.



- Why does Blockchain matter to create trust? Possible answer to

“how can you trust people that you don’t know?“

Review of blockchain's core benefits and risks

Key Benefits

- Permanent, transparent ledger enables increased **transparency** and **auditability** while **reducing risk of data loss** or conflicting records
- High divisibility of 'units' facilitates fee-less **micro-transactions**
- Higher **efficiency** and reduced friction through the elimination of centralized authority for P2P interactions **lowers transaction costs**
- Public or private, depending on the blockchain protocol, with customizable permissions allowing **sensitive data** to be managed
- Identifiable and programmable units enable **smart contracts** for more effective management of digital assets and offline P2P agreement
- **Elimination of single points of failure** and reduced need for trust

Primary Concerns

- Variable throughput capacity between blockchain protocols suggests an **uncertain scalability**, and potential concerns over transaction **latency**
- Possible consensus protocol flaws, i.e. in the event of malicious agents on the network, may result in a **lack of complete asset security**
- Uncertain **regulations** in certain use-cases, particularly those handling sensitive assets such as healthcare, securities settlement, and contracts
- High deployment **costs**, particularly in data sensitive, complex data operations, may prove an inhibiting factor in blockchain adoption, and at the very least extend the timetable for deployment
- Shift from centralized authority to an autonomous, digital, and decentralized network for trusted P2P transactions **challenges societal and industry norms**, and may face sharp resistance
- **Irreversible** transactions (e.g. the DAO hack)

Blockchain: potential for great things

secure

monetize

- Monetization
  - Blockchain: enable the creation of decentralized digital curency (i.e bitcoin or other cryptocurrencies)
  - Blockchain enables to perform low cost microtransactions required in many IOT application (i.e energy)
- Security
  - Autorisation and Access control is required in many blockchain applications
  - Fortified security platforms such as authorization and access control may be replaced by blockchain applications
    - Minimize the cost of security
    - Spread the risk
    - Eliminate single point of attacks

Blockchain enables to move from a « strong » to a « weak » trust manager model

Bitcoin
Governance
SmartProperty
Voting
SmartContracts
Name Registration
Identity
Crowdfunding
IoT
Climate

And as a matter of conclusion: what are the (big) problems we have to solve ?

- Connected objects
  - Combination between massive IoT + local computing power + network connectivity => transformation of all connected object from our day to day live could give birth to an un-precedented set of usages **and threats .**
  - **Mirai is just an appetizer!!!**

- Big-data issue
  - In 5-7 years time frame it will be possible to provision for AI/analytics purpose about **10 PB of data in less than one hour**
  - Fine for legitimate organizations
  - **What does it imply for structured malevolent organizations or governments?**

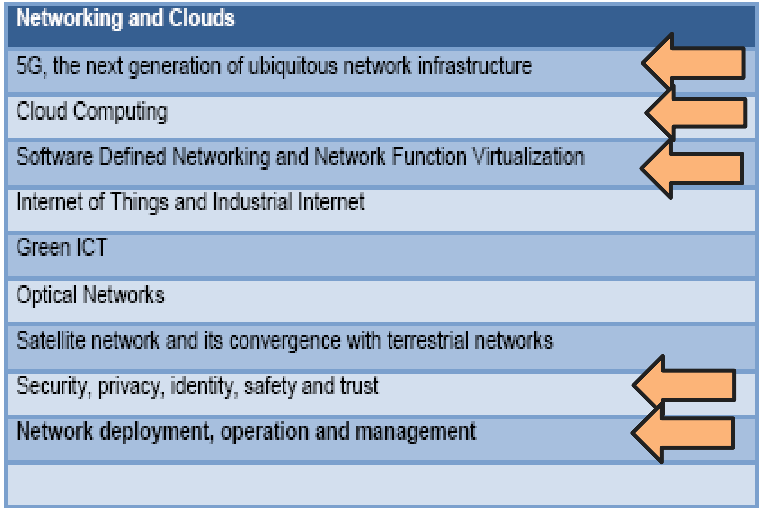
Some Hints: it's before all a matter of trust & also Research

- More regulation for suppliers: towards a (European) IoT label or set of labels?
- More constrained framework for device OTI/OTA update or replacement

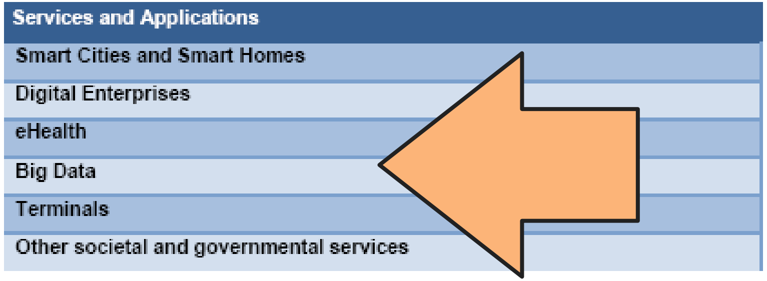
- Towards a more prescriptive consumer information?

- Building/extending (neutral) silos of accessible(big) IoT data suitable for analytics, serious games, simulation, research on weak-signals,..
- Building/extending set of guidelines, best practices, dictionary of threats/counter-measures, incidents…. available

- Start building extensive test sets, suitable for given parts of IoT architecture (end-devices, gateways, ..)



Networking and Clouds
5G, the next generation of ubiquitous network infrastructure
Cloud Computing
Software Defined Networking and Network Function Virtualization
Internet of Things and Industrial Internet
Green ICT
Optical Networks
Satellite network and its convergence with terrestrial networks
Security, privacy, identity, safety and trust
Network deployment, operation and management



Services and Applications
Smart Cities and Smart Homes
Digital Enterprises
eHealth
Big Data
Terminals
Other societal and governmental services

Thank you! Have a safe journey in the IoT!