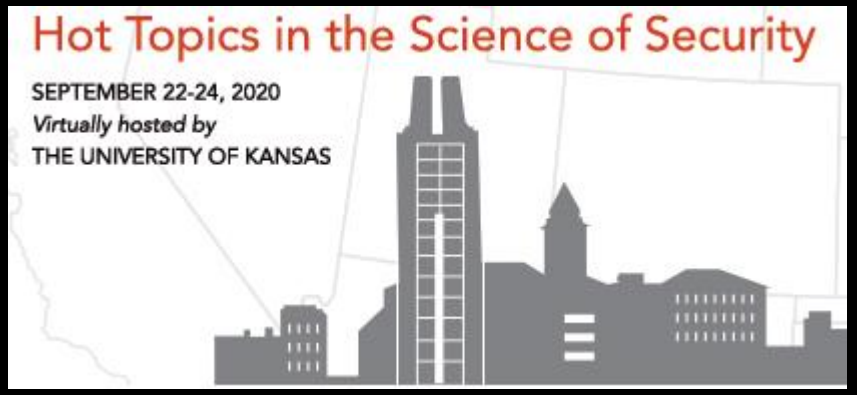
HotSoS 2020

Lyle Paczkowski
T-Mobile Advanced and Emerging Technology
23 Sept 20
V4

Agenda

- Quick Introduction
- Current state of technology trajectories - 5G influence
- The Supply Chain
- IoT - Future state of the “Security Problem, and the Solution”
- The prediction of next phase of the “secure system”



The Science of Security (SoS) emphasizes the advancement of research methods as well as the development of new research results. This dual focus is intended to improve both the confidence we gain from scientific results and also the capacity and efficiency through which we address increasingly technical problems.

A little about T-Mobile…

T-Mobile is the undisputed growth leader in wireless and business enterprise solutions

- **98.3 million**
  customer base
- **$17.7 billion**
  2Q total revenue

We have good stuff….

Now #2

(overtaking AT&T)

Business is changing

Business growth used to come from scale. Now it comes from agility, intelligence, and the ability to deliver better experiences.

Today, all companies are technology companies. That's because all companies are driven by constant technological innovation.

And much of this technology requires mobility — powered by advanced wireline and wireless networks.

The Global Community – the real situation

- Fragmentation of thought in the early stages of 5G design, services, and protocols
- Too few levels of standardization are defined across the board – particularly IoT
- A plethora of use cases, some of which might be impractical
- A HUGE market to secure and protect, with few legitimate ecosystem methodologies (Layer 7 security isn't good enough)
- Telecom is moving to Datacom

General Discussion topics

- Is Security at layer 7 good enough? How do we make it more secure?
  - Hardware Root of Trust (PSA and the GSA)
  - Blockchain and Hyperledger
- Data is the Enterprise primary asset. Logistics, supply chain, inventory control are problems that are difficult to solve without an integrated approach.
  - How could a 5G "Near Cloud", with Hyperledger (A form of Blockchain), solve for these significant corporate challenges?
- 5G and what it means – physical vs. logical
  - What is the SCEF business conduit? And, how will this affect us and our customers in a new and interesting ways
  - What is network slicing in 5G and how will customers be able to become a slice? What would this accomplish? What monetization trail could be realized once this is in place?
  - Orchestration and virtualization are two main business drivers for 5G. What will this do that couldn't be done in any prior "Gs"
  - What does it mean to "be able to use a carrier network as if it were their own?"
- IoT is the next evergreen opportunity

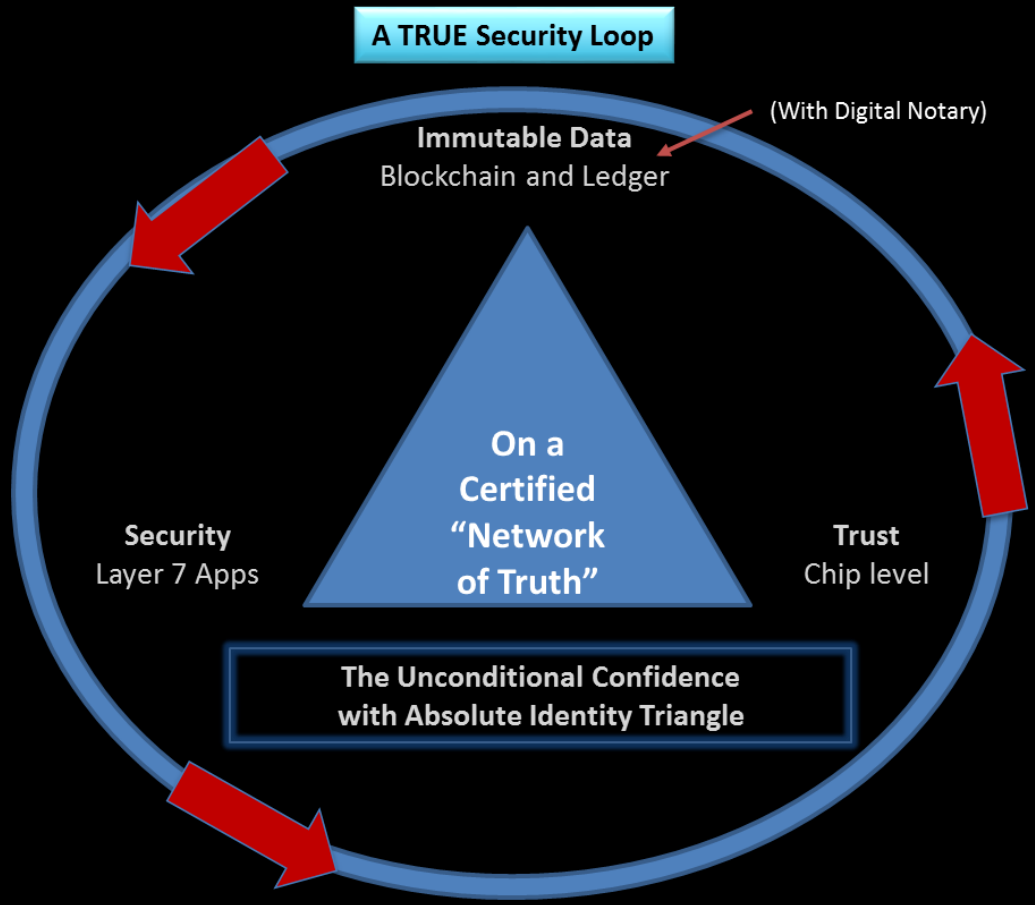
Issues - Problems – Concerns
Is anything secure in the current environment?

- **IoT – The "Inventory of Things" is current state**
  - The "Internet of Things" is a future state
- **Absolute Identity**
  - True Identity suggests un-hackable identity
- **Extensions of Security**
  - Hardware Root of Trust and Hyperledger
- **Years to Quantum (Y2Q)**
  - Should we be concerned?
- **Global and National Ledger Alliances**
  - Lots of engagements looking to help solve for security

Feeling Secure and Being Secure should correlate

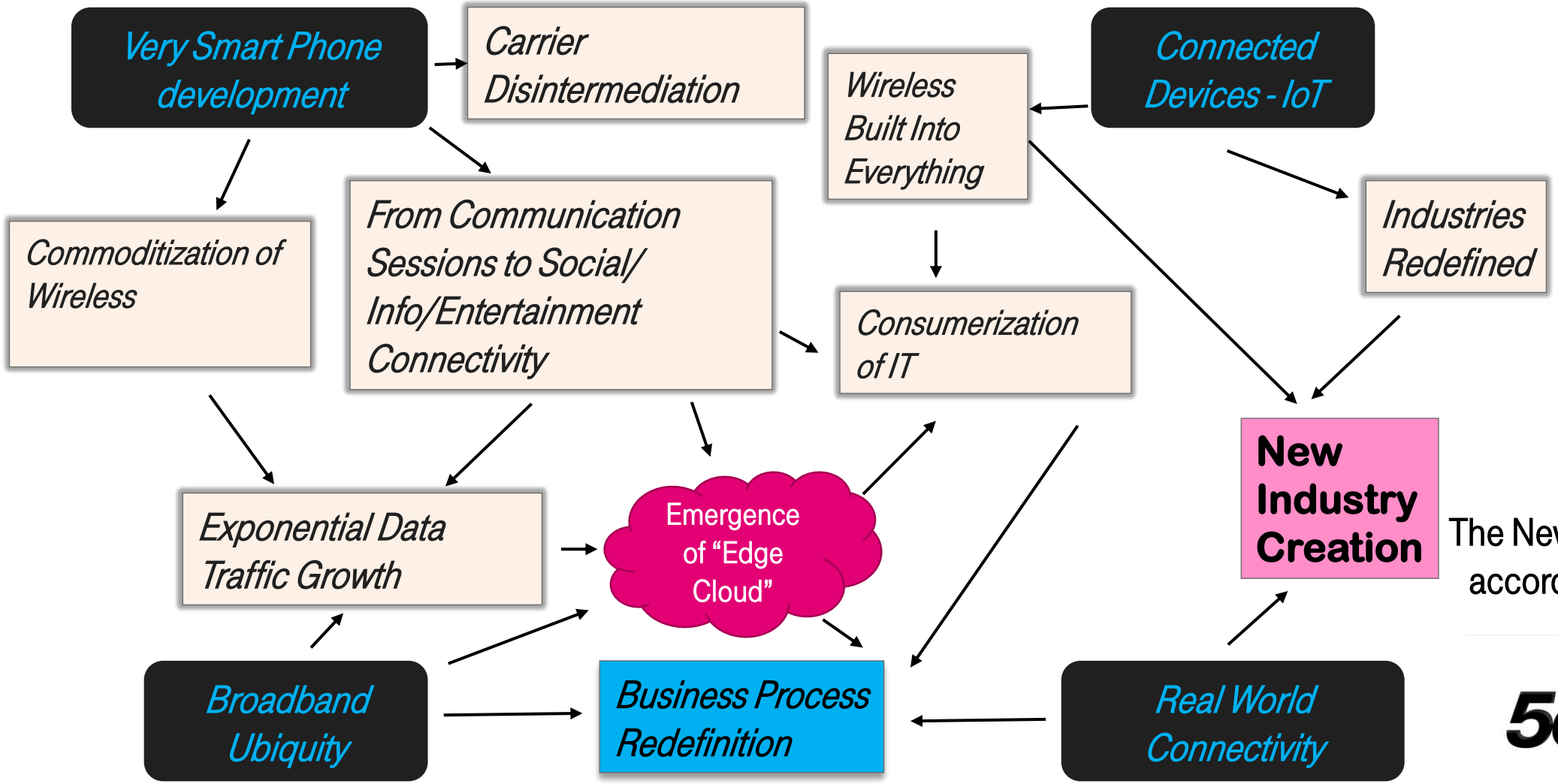
Inventory, True Security, Absolute Identity

- Too many appliances, not enough individual secure identifiers
- Carbon-based ID VS. Silicon-Based ID
- Identity that is Reference based, decentralized, and bombproof
- Ledger is an extension of Security, and Identity (mostly)
- Hardware Root of Trust is not widely understood, nor widely deployed



Blockchain and Distributed Ledger Technologies are an extension of Security

Ten Critical Business / Technical / Industry Shifts due to 5G



The New World according to

5G

The Wireless Ecosystem Influence Matrix
The "Connected Compute" Reality

Ability to dictate in an un-fragmented handset market

Ability to dictate in a FRAGMENTED IoT market

Moderate influence	Wireless Network	Unlicensed Wi-Fi (Unsecure) / Licensed Spectrum (Secure)	High influence
		Inside / Outside	
		OEM	
No influence	Operating System Stack	Linux, Windows, iOS, Android	Total influence
		ODM	
Some influence	IP Base	ARM, ARM TrustZone, Intel, Trusted Computing Group	Moderate influence

New value propositions that drive Trust

- Principle of Consistency
  - Run Time Integrity Checking
  - On all-data networks it is critical to watch for executable discipline
  - Enterprise SLAs are now demanding forms of uniformity (app market products are not uniform)

- Principle of Indemnification
  - "Access" is the new "luxury"
    - If this is true, then Security is the new commodity.
  - Collaborative consumption will demand Peer to Peer
  - Access to anyone from anything is demanded
  - Person to person commerce happens where individuals are both buyers and sellers of goods and services.
- Yields "perfected compensation"
- End to End transactions must exhibit a *Continuum of Trust.*

Both Arm and Intel are devoting time and money to expand the IoT ecosystem.

Use Cases for On-device Processing

As AI mainstream popularity grows, so does the range of applications businesses seek to develop. These fundamental use cases are inspiring companies of all sizes to innovate for new possibilities and disrupt existing markets.

Vibration and Sensor Fusion

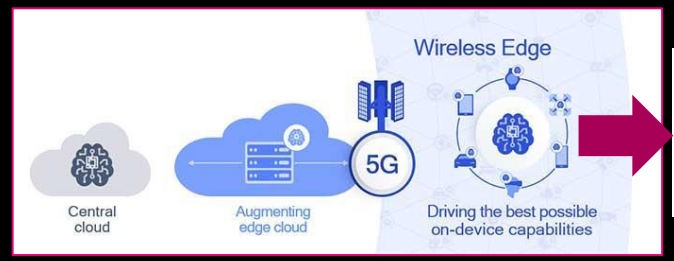
Wearable health tracker, industrial sensors, motor control, industrial anomaly detection.

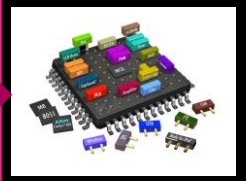
Voice and Sound

Voice-activated home devices, such as smart speakers, and lightbulbs, headsets and earbuds.

Vision and Image

Video doorbell, gesture-controlled machines, smart door unlock, quality assurance.





One more icon will eventually be added to this image – Network on Chip

Hardware, Software, Tools and Ecosystem Provide Best-in-class Solution

The combination of leading hardware IP, easy-to-use tools, open source software and leading ecosystem are enabling AI for IoT to scale.

Additionally, Arm's comprehensive, full-stack suite of integrated software and tools make it easier and quicker to design, develop, and maintain AI-based IoT applications. Read the Blog

Cortex-M55 Processor

Arm's most AI-capable Cortex-M processor delivers enhanced, power-efficient digital signal processing and machine learning performance.

Learn More >

Ethos-U55 microNPU

The industry's first microNPU for Cortex-M, specifically designed to accelerate machine learning inference.

Learn More >

Corstone-300 Reference Design

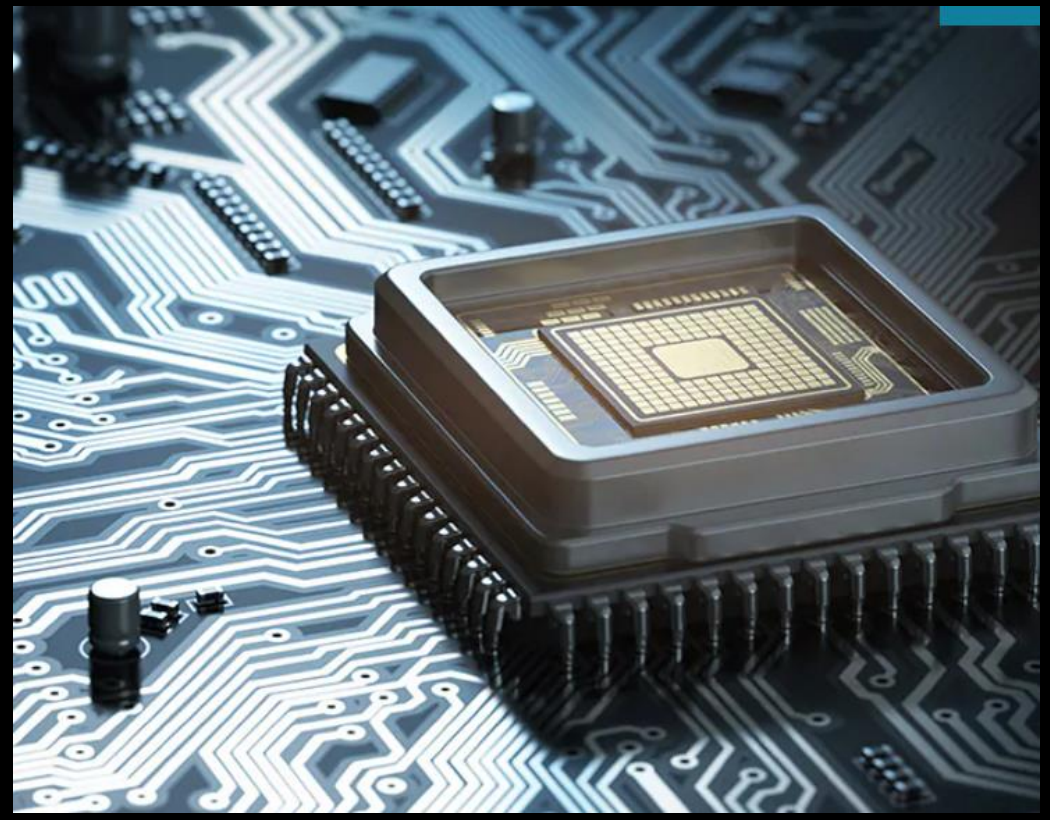
The fastest way to incorporate the Cortex-M55 and Ethos-U55 processors into a system-on-chip design.

Learn More >

5G can support up to a million devices per square kilometer, while 4G supports only up to 100,000 devices per square kilometer

Chip to Chip, Chip to Cloud, Mouse to Mouse

"Securing the Internet of Things (IoT) is not something that one company or entity can achieve alone. Arm believes that *security is a shared responsibility* and should be embraced by the whole ecosystem, from chip to cloud.



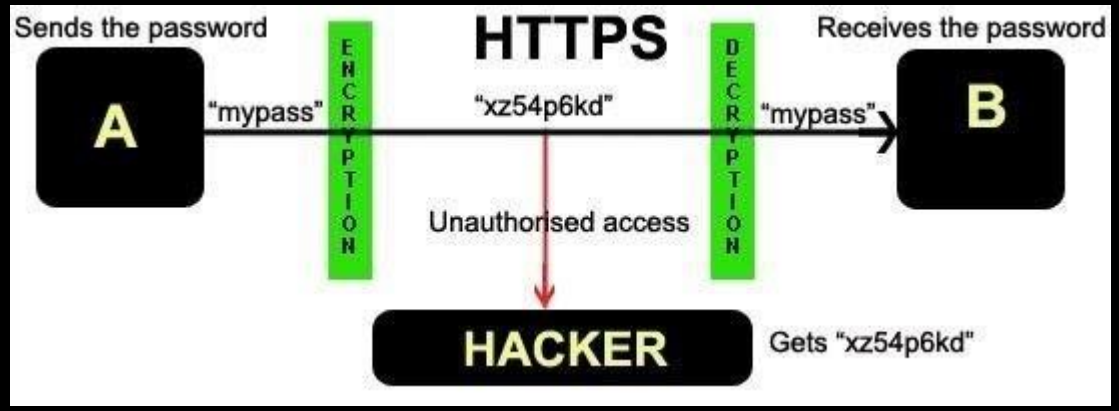
Platform Security Architecture (PSA)

- The PSA - ensure that security is designed into a device from the ground up. The four implementation stages:
  - Analyze: the evaluation of assets and assessment of threats to define specific security requirements.
  - Architect: the security design based on identified security requirements.
  - Implement: an open source firmware implementation that complies with the specifications from the architect stage.
  - Certify: assurance that products adhere to security requirements and PSA guidelines, through the PSA Certified scheme.

Communication Vulnerabilities

Attackers can try multiple means to intercept, spoof or disrupt messages sent from devices back to the server.

Best-practice cryptographic defenses must match the increasing value data being communicated.

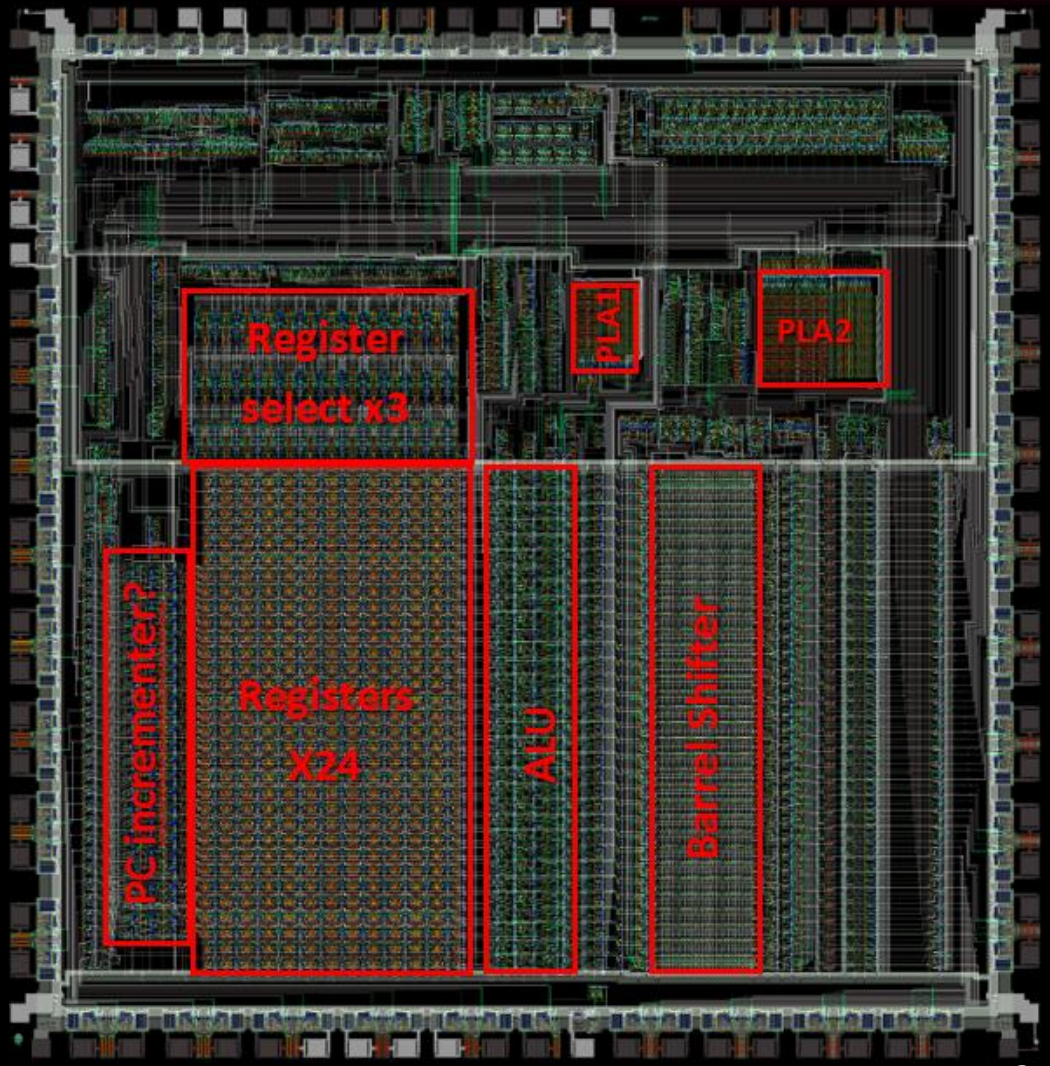


Physical Vulnerabilities

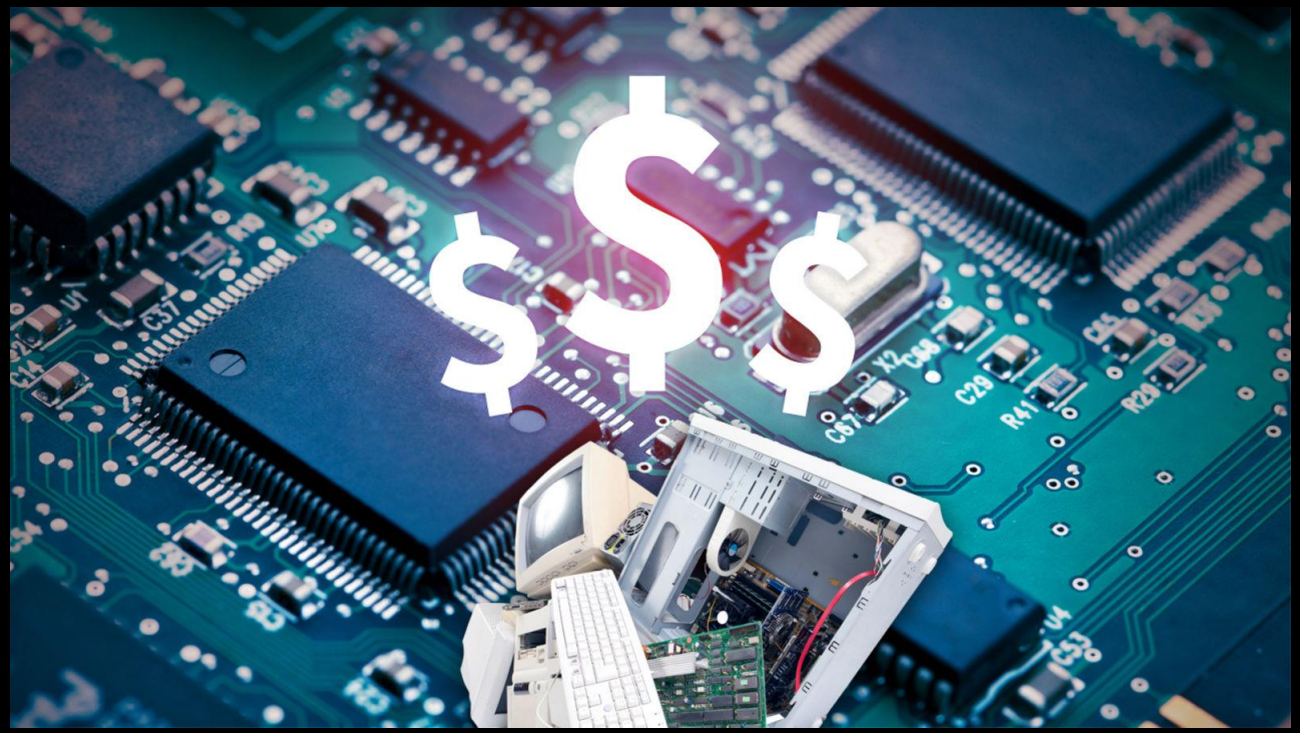
Silicon attacks are often split into two categories: non-invasive and invasive.

Non-invasive (side-channel) use different ways to try to observe the chip to gain information. These include perturbation techniques–altering the power supply voltage or interfering with electromagnetic signatures.

Invasive techniques involve opening the chip to probe or modify part of the passivation layer.



Lifecycle Vulnerabilities



Devices changes hands many times—from factory to user, to maintenance and to end-of-life.

The integrity of the device must be protected at each step: who is repairing it, how is confidential data handled, are firmware upgrades legitimate.

Unplanned or forbidden paths, such a theft, overages, or Wi-Fi changes are all vulnerabilities to consider.

Software Vulnerabilities

These are the most common attacks where someone finds a way of using existing cost to get access to restricted resources.

It could be due to a software bug or to unexpected call sequences that are open to whole classes of exploits.

Platform Security Architecture framework
Three levels currently specified…

Current

PSA Certification group: ARM, Brightsight, CAICT, Riscure, Prove&Run, Underwriters Lab

Possible NEW Fourth level added to PSA?

psacertified™ level one

Security model based

critical security questions

with lab interview

For Chip vendors

For OS suppliers

For OEMs

psacertified™ level two

Lab based evaluation of the PSA-RoT

Mid assurance & mid robustness

For Chip Vendors

psacertified™ level three

Lab based evaluation of the PSA-RoT

Substantial protection from software and hardware attacks

For Chip vendors

psacertified™ leve FOUR

Hosted Remote Kernel measurement of Trusted Processors with Audit and Indemnification attributes

The most urgent system that requires Trust and Secure data …

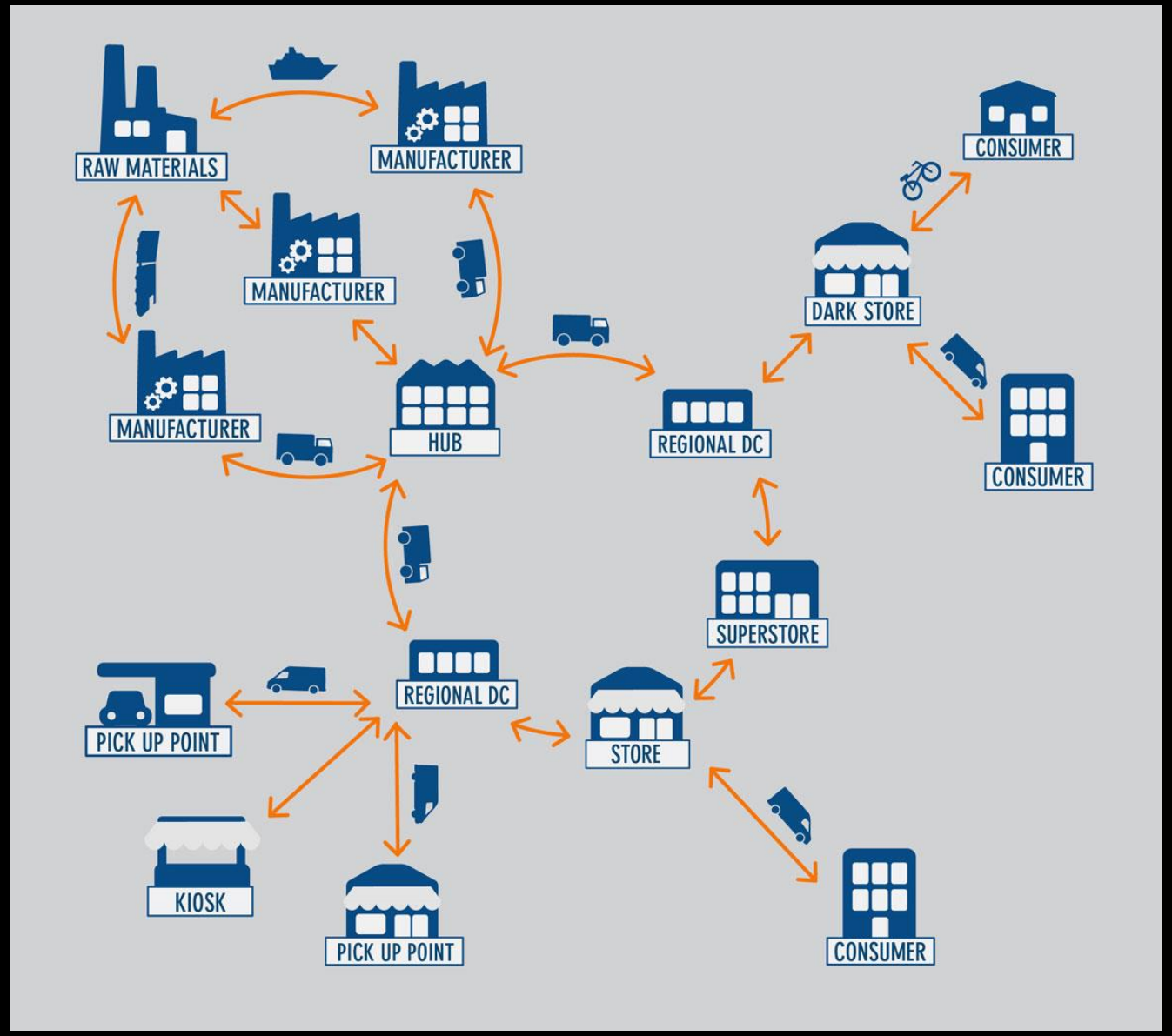
…including the notion of ‘true identity’?

The Supply Chain!

Hardware root of trust is part of the answer…

For many intelligent edge devices, especially devices that can be physically accessed by potential malicious actors, hardware security is the last defense for protection.

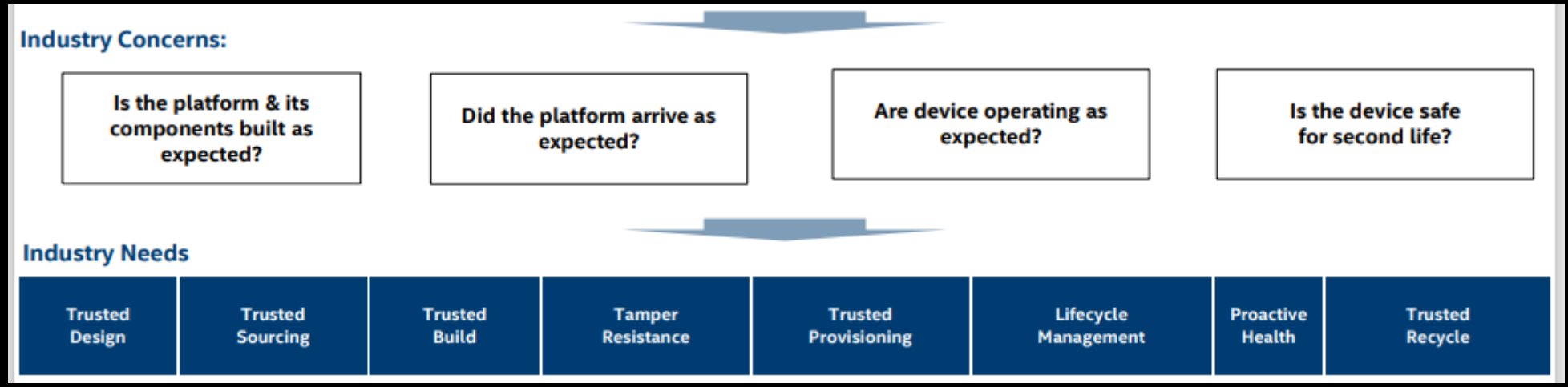
True Identity, plus tamper resistant hardware, is crucial for such deployments.



Trusted Supply Chain initiative

Problem
- Assurance of a device's origin in today's diverse manufacturing, logistics, and just in time inventory
- Remote deployment and provisioning requires assurance in the Supply Chain.

Solution
- Use a Root of Trust to provide assurance of a device's origin
  - This Root of Trust establishes the foundation for a Trusted Supply Chain (TSC)
- Blockchain adds an additional layer of trust in the overall system supply chain



Basic Transparent Supply Chain Process

GENERATING THE CHAIN OF TRUST BASED ON TRUSTED PLATFORM MODULE

Trusted Platform Module Manufacturer

- ***Creates Endorsement Key*** (EK) for each Trusted Platform Module (TPM)
- Establishes **hardware root of trust**

System Manufacturer

- Permanently ***mounts TPM*** onto motherboard
- ***Creates platform certificate*** and binds it to the EK

System Integrator

- ***Creates appliance certificate***
- binds it to the platform certificate

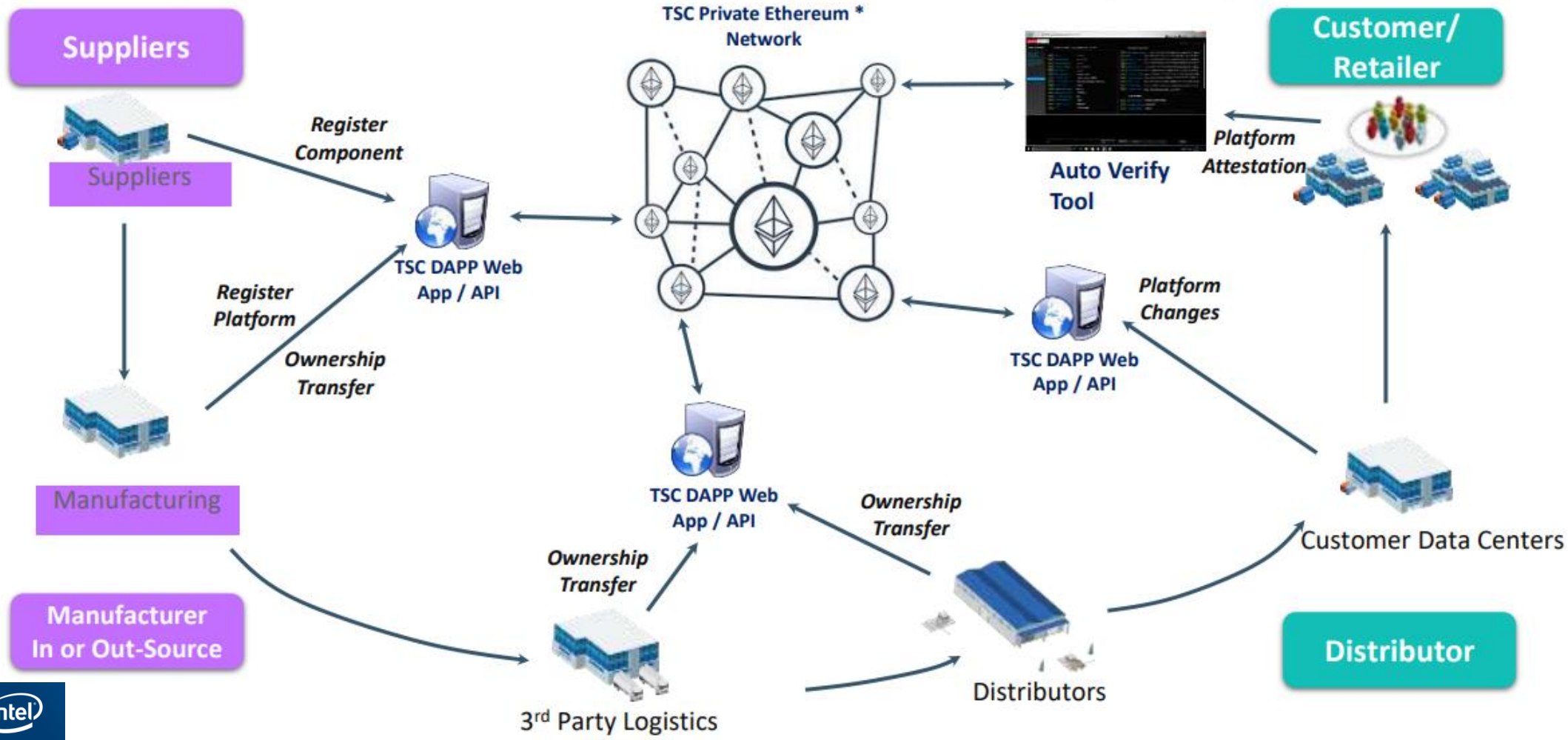
IT Department

Platform Certificate Verification Tool

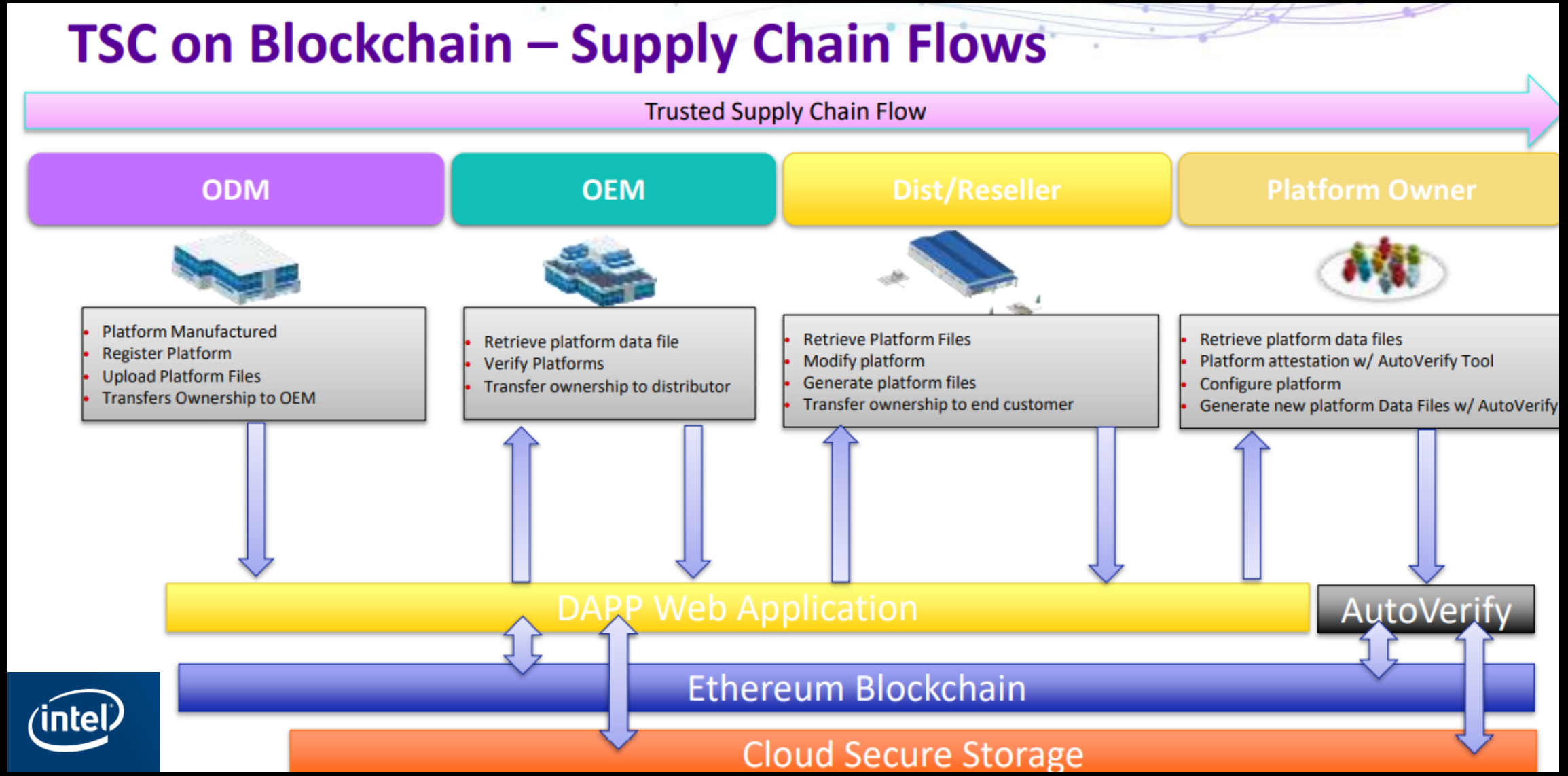
- *Verifies the **Platform Cert** against the platform*
- *Attests to the **Root of Trust** to the End User*

Chain of Trust Built Up by Multiple Parties in System Lifecycle

TSC on Blockchain



TSC on Blockchain – Supply Chain Flows



The new big deal - 5G

5G – “People and Things brought together”

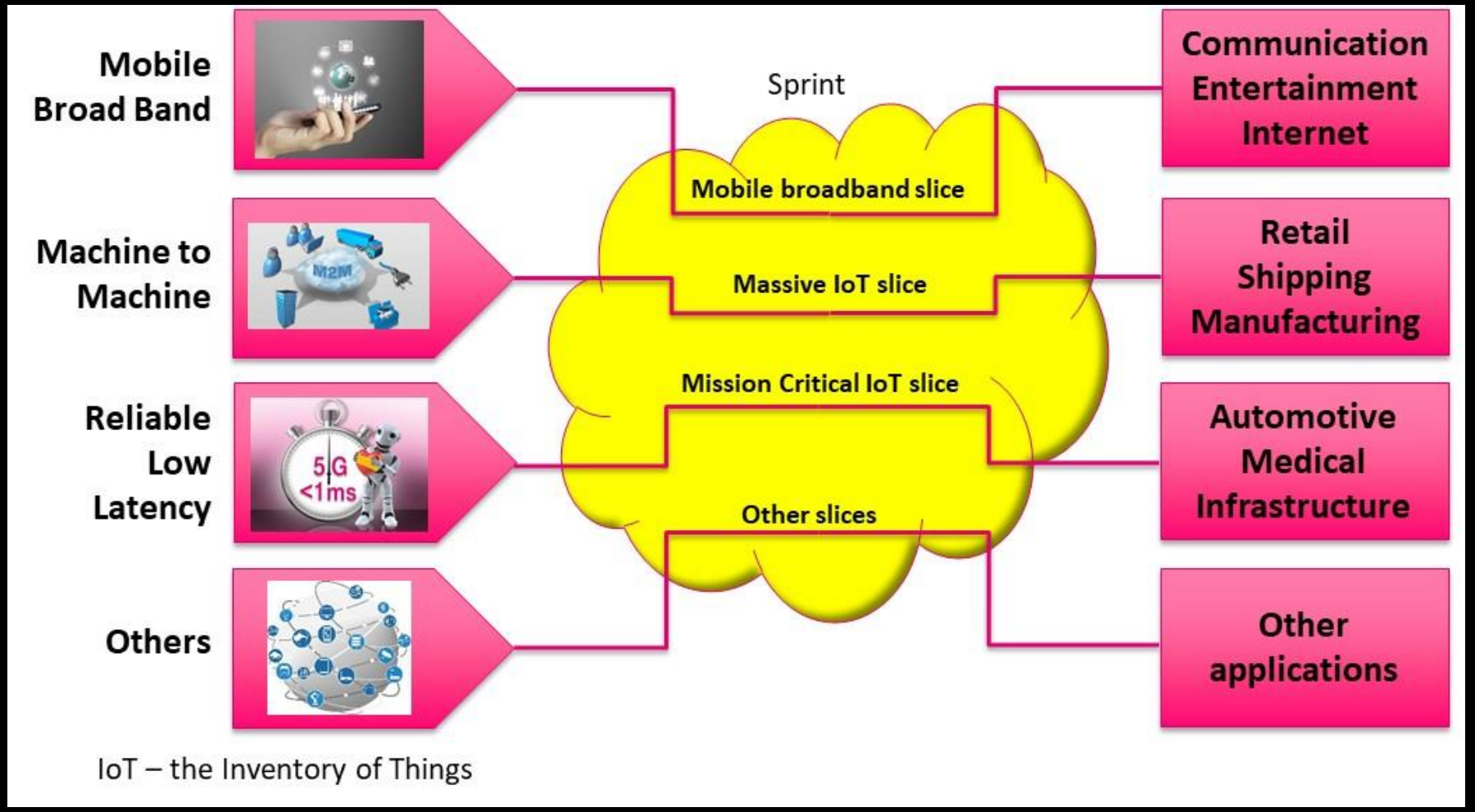
5G networks will be built around people and things, and will natively meet the requirements of three groups of use cases (Slices):

1. Massive broadband (xMBB) that delivers gigabytes of bandwidth on demand
2. Massive machine-type communication (mMTC) that connects billions of sensors and machines
3. Critical machine-type communication (uMTC) that allows immediate feedback with high reliability and enables for example remote control over robots and autonomous machines, or “URLLC”

“Network softening” includes the ***orchestration*** of network functions in software, the ***virtualization*** of these functions, and the programmability by establishing the appropriate interfaces – ***containerization***

5G Network Slicing

Slicing enables service providers to build virtual end-to-end networks tailored to application requirements



Network Function Virtualization (NFV)

- Harmonize
- Containerize
- Orchestrate

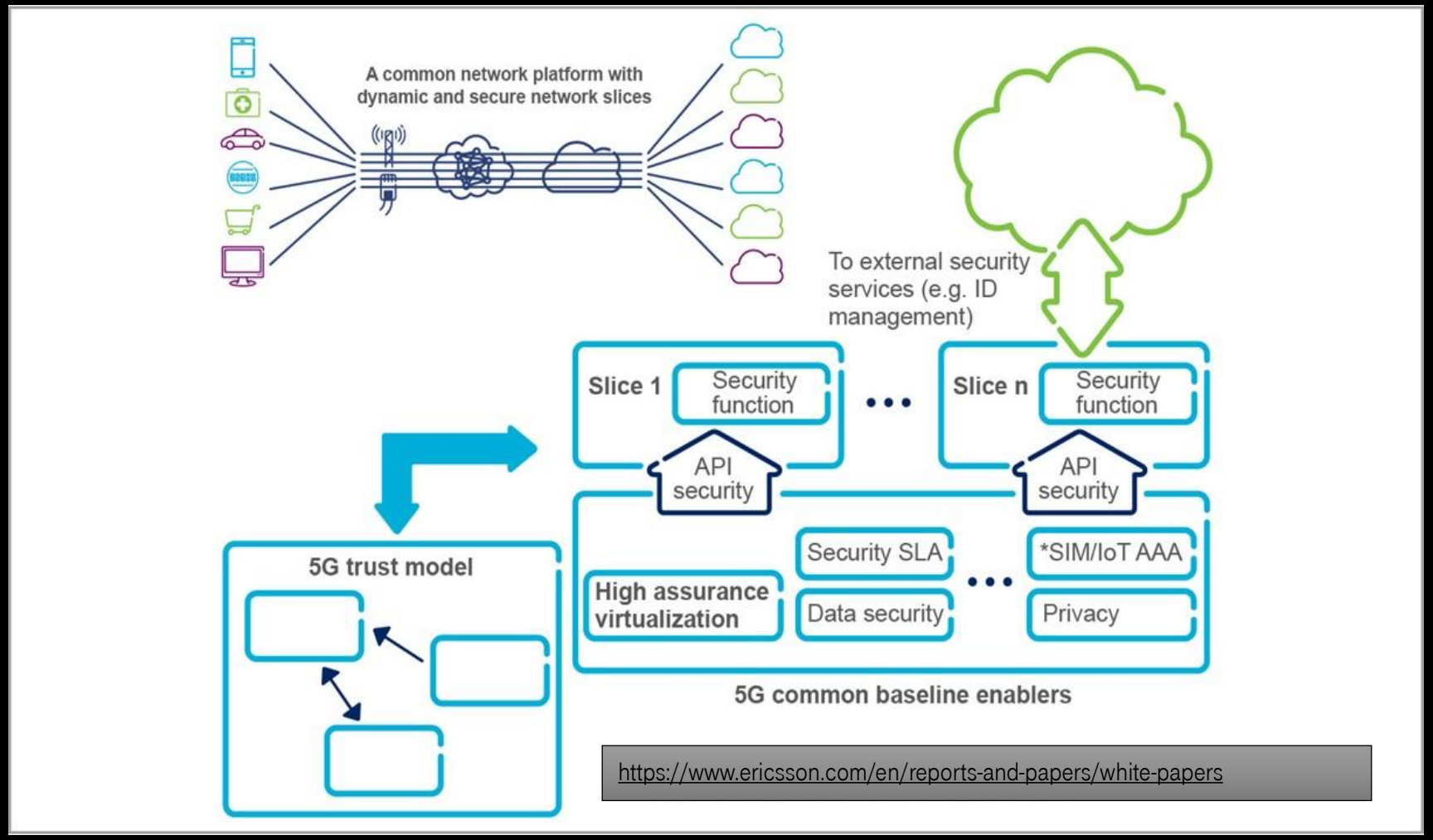
Virtual Network Functions (VNF)

- Working elements

How to secure?

5G Slice Security

Network slicing (a VNF) is evolving to become one of the most beneficial and desirable future Business Enterprise capabilities resulting from 5G (Rel 16)

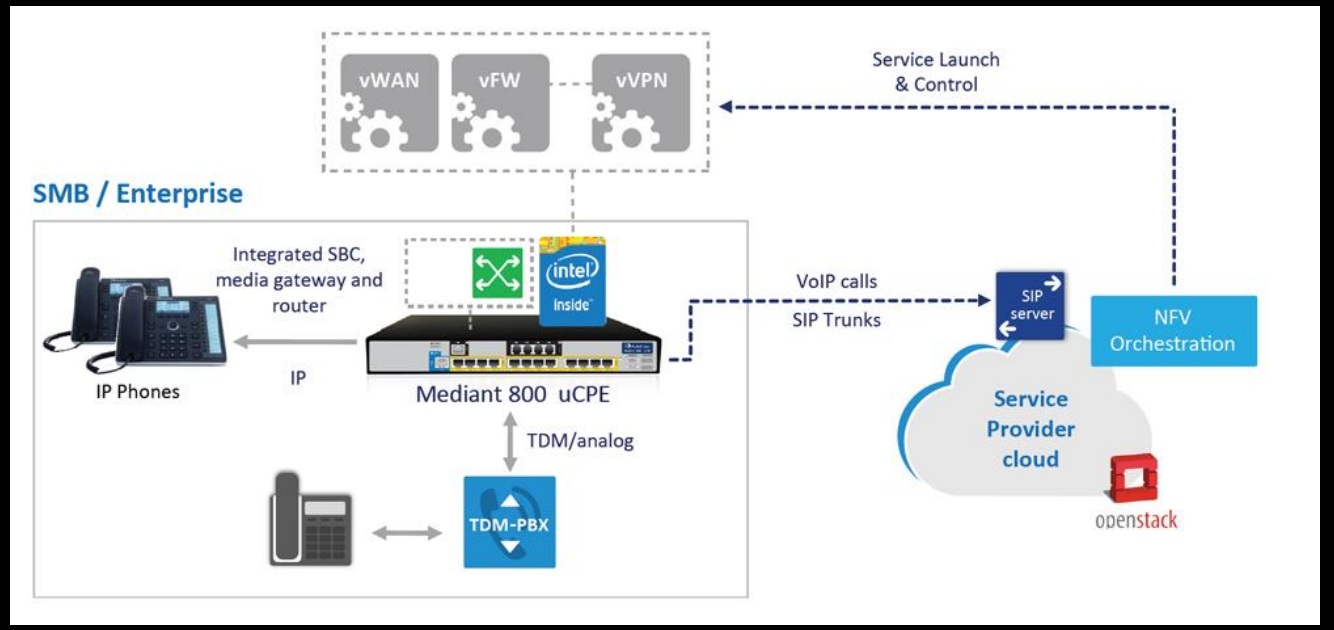


Impact of edge computing

A major headache for many within the IoT ecosystem is how to manage security as more and more devices are connected.

Malware can be used to harness IoT devices to perform DDoS attacks.

While edge computing is unlikely to be more secure than a private cloud, it does have the benefits of being more local.



For companies concerned about storing data in locations which, for example, have different data protection laws than where the data is being generated, edge computing can provide some security benefits.

This fly's in the face of the Business Enterprise “moving everything to the Cloud”.

Another emerging problem:
Too many Things, not enough IDs

And, Networks and Things can learn (mostly)
But
Can they Think?

Secure Machine Learning and Secure Machine Thinking can only be the future state

Identity – Future State?

Carbon Based Identity

And / Or

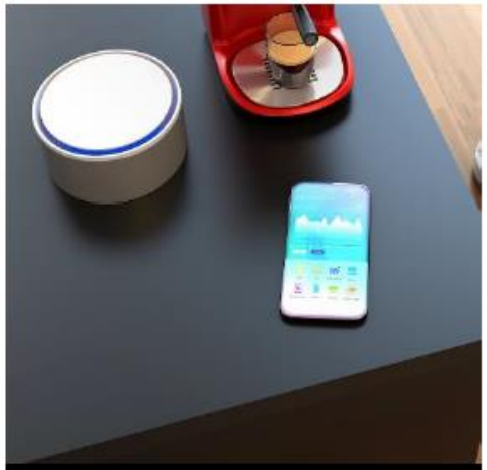
Silicon Based Identity

Network Identity formats today are generally based upon network access (IMSI), discoverability, and data subscription plans via NPA-NXX - the telephone number.

How would YOU fix it?

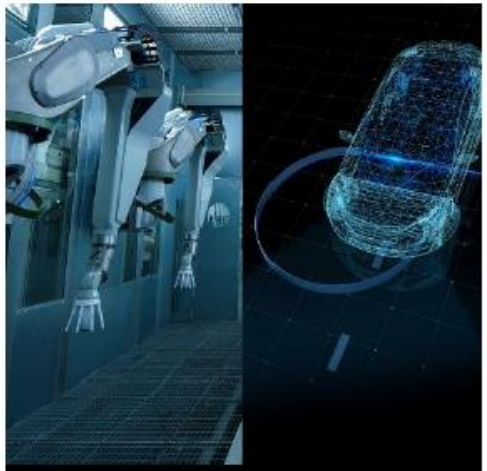
Technology trends that will redefine all industries

Assimilated Intelligence



Artificial Intelligence in every device

Connected Machines



Autonomous machines

Reality, Augmented

Augmented reality

The Near Cloud

Hyperscale cloud and connectivity

Security and Privacy

WORKING LIFE

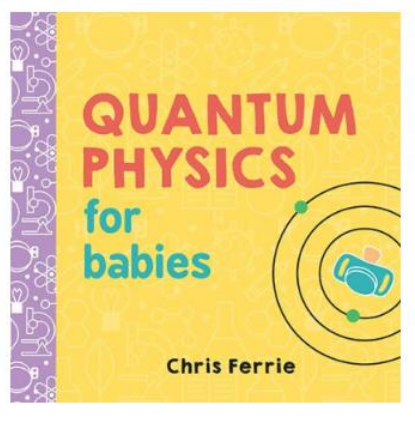
Quantum computing is on cusp of commercial breakthrough

A Cambridge start-up's operating system could lead to the creation of a software market

The thought experiment of Schrödinger's cat, and whether it can be dead and alive at the same time, is an analogy for the "superposition" inside a quantum computer

ALAMY

https://www.thetimes.co.uk/article/quantum-computing-is-on-cusp-of-commercial-breakthrough-8tgjjfsqj



Recommended reading

Key take aways…

- 5G will transform your business and, “you will be able to use our network as if it were your own”
- Data is the new oil, and is the principal business asset to protect – the security problem
- Identity, carbon based and silicon based, becomes the ultimate security objective
- Supply chain will be the most significant affected business process
- The speed of the connection will create significant new opportunities
- Distributed data shares will begin to become standardized IE: IPFS

In Closing….


Thanks to: Perry Alexander (The University of Kansas)
And the Program Co-Chairs: Baek-Young Choi (University of Missouri – Kansas City) and Drew Davidson (The University of Kansas)
for inviting me.
Lyle.w.paczkowski@t-mobile.com