Connected Living Programme

oneM2M March 2015

Program activity update

CONNECTED LIVING – ACTIVITY UPDATE

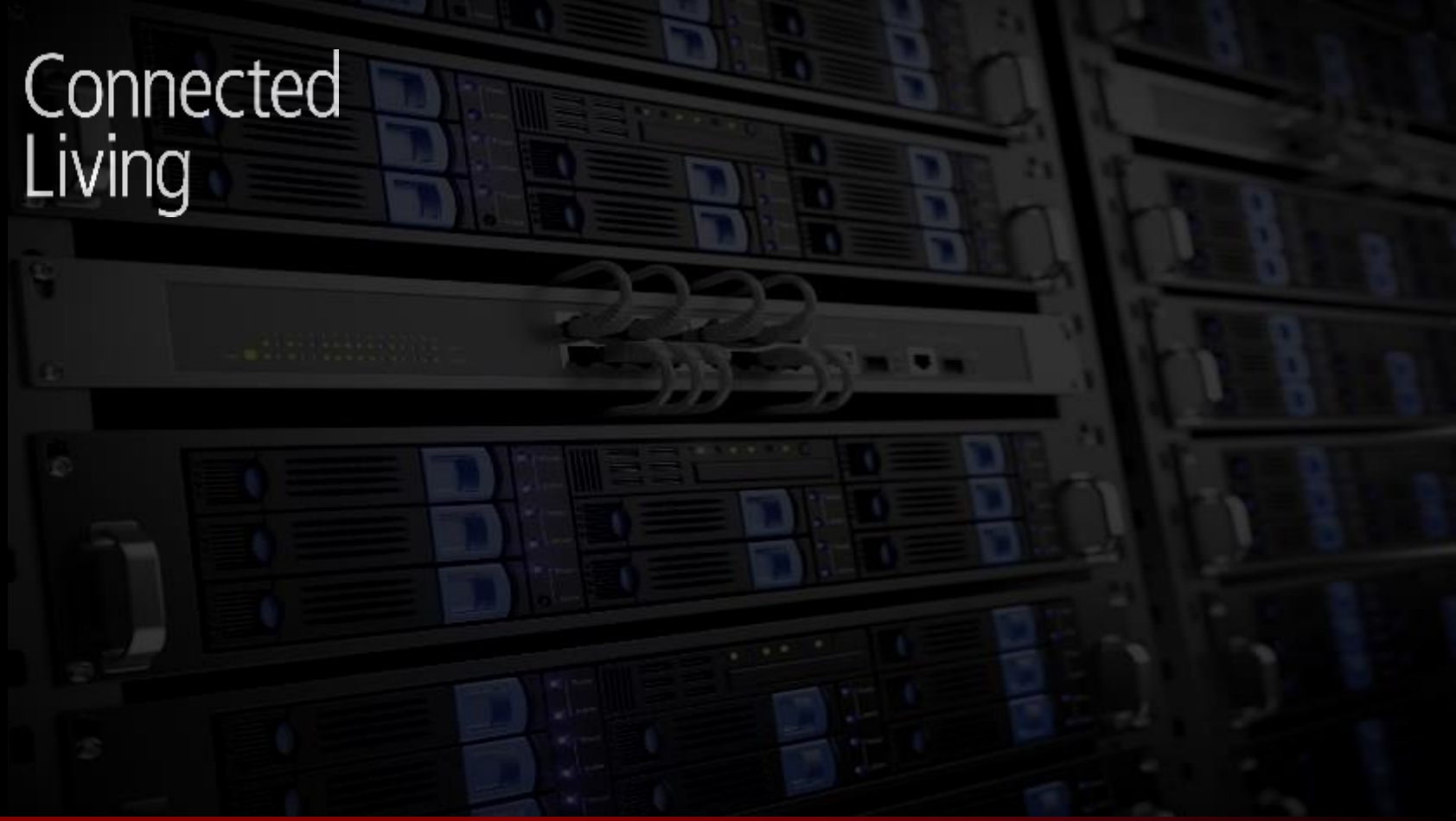
IoT CONNECTION EFFICIENCY

- IoT Connection Efficiency Guidelines Version 1.1 published. This version adds ‘Device Host Identity Reporting’ (DHIR) capability to the guidelines
- IoT Connection Efficiency Test Cases Version 1.0 published. Version 1.1 will be published in April 2015 (to add DHIR test cases and add further clarification of the intended test environments)

CONNECTED LIVING – ACTIVITY UPDATE

IoT SECURITY

- CLP.04 End-to-End Security for M2M & IoT position paper
- CLP.06 End-to-End Security for M2M & IoT Whitepaper
- New work to produce End-to-End Security guidelines, all GSMA members are welcome to join



IoT CONNECTION EFFICIENCY

Connected Living Programme

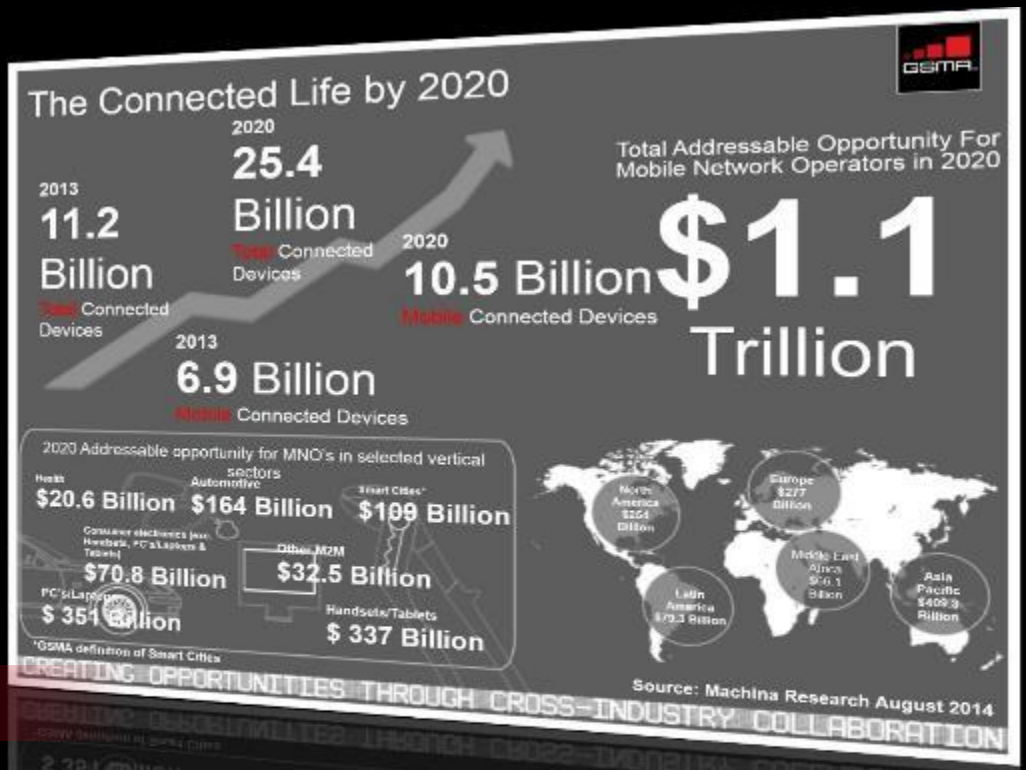
OVER TO OUR PARTNERS…

Here's what some of our partners have to say……

PROBLEM STATEMENT

THE GROWTH OF IOT DEVICES AND APPLICATIONS WILL CREATE MAJOR CHALLENGES FOR THE IOT ECOSYSTEM:

- Local issues e.g. cell congestion.
- Capacity and performance problems within the core network.
- Degradation of the IoT service's performance.
- Increased power consumption of the IoT devices.



HOW CAN THIS BE AVOIDED?

WHAT CAN GO WRONG?

#1 Local area network congestion due to poor application design

- In Mumbai all school buses are connected devices.
- When the buses are geographically distributed around the city the data traffic generated is consequently distributed across the mobile network operator's network.
- However, when the buses return to the bus depot at then end of the day the data traffic becomes concentrated onto a small number of cells within the mobile network causing network overload of these local sites. This congestion then affects all the other mobile network users in this local area.

HOW COULD THIS HAVE BEEN AVOIDED?

WHAT CAN GO WRONG?

#2 Fraud due to Insecure IoT Communications Modules

- In this case, the operator's B2B customer had an installed base of 59 IoT devices used to monitor wind and solar power generation.
- A hacker had discovered the temporary public IP addresses of the IoT devices and then logged on to each device using the default username and password.
- In December 2013 17,000 fraudulent voice calls were made by the 59 IoT devices to Gambia, Latvia, Lithuania, UK and the Falkland Islands.

HOW COULD THIS HAVE BEEN AVOIDED?

WHAT CAN GO WRONG?

#3 Network Overload due to Unintelligent Error Handing Mechanisms

- An European operator's B2B customer had an installed base of approx. 375,000 geographically fixed IoT devices (for use in the homes of consumers).
- In 2013, the customer's server suddenly and unexpectedly stopped acknowledging the status reports from the IoT devices. This error caused all of the devices to reboot every few seconds to try to re-connect to the mobile network inadvertently creating a 'denial of service' attack.
- Overall, it took this operator approximately 48 hours to completely resolve the problem which classified the event as 'critical' on their network.

HOW COULD THIS HAVE BEEN AVOIDED?

USE OF GUIDELINES WITHIN BROADER ECOSYSTEM

- Should work with their developer partners to implement the requirements contained within the guidelines.
- Should reference the guidelines in the supply contracts they place with their developer partners.

- Should ensure that their communication modules conform to the requirements stated within the guidelines

- Should ensure their IoT services and devices conform to the requirements stated in the guidelines.
- Should reference the guidelines in the supply contracts they place with their IoT device makers

- Should ensure that their IoT device application conforms to the requirements stated within the GSMA connection efficiency guidelines.

- Should promote the use of the guidelines.
- Should make commercially reasonable efforts to reference the guidelines in the connectivity contracts they agree with their IoT Service Providers.

- Should ensure that their radio baseband chipsets conform to the requirements stated within the GSMA connection efficiency guidelines

KEY FEATURES DEFINED WITHIN THE GUIDELINES

Network Friendly Mode

- Network Friendly Mode is a non-standardised feature of the Communications Module that polices the amount of times the Communications Module can perform IMSI attach, GPRS attach, PDP Context activation and SMS-MO in order to reduce the amount of signalling generated towards the HPLMNs HLR, SMSC or GGSN.

Radio Policy Manager

- Radio policy manager is a radio baseband chipset feature that protects the Network by performing “Connection Aggression Management” which is necessary when a device is aggressively trying to access the network following various NAS reject scenarios.

KEY FEATURES DEFINED WITHIN THE GUIDELINES

- **Device Host Identity Reporting**
  - Mechanism to identify the host device which contains the Communication Module.

TEST CASES

- **A companion set of test cases was delivered in January 2015**
  - The document outlines the test cases that would need to be passed by an IoT Device and its incorporated Communications Modules in order for it to be considered compliant with the requirements stated within the GSMA's IoT Device Connection Efficiency Guidelines.
  - The target audiences for this document are Mobile Network Operators, IoT Service Providers, IoT Device makers, IoT Device Application developers, Communication Module Vendors and Radio Baseband Chipset Vendors.

WHAT IMPACT ARE THE GUIDELINES HAVING ON THE MARKET"

"Telit believes that the GSMA's Connection Efficiency Guidelines do a very good job of preventing service degradation and other problems that could surface with the massive growth expected from the IoT and where M2M modules play a key role."

Marco Stracuzzi, Product Manager, Telit

"Qualcomm is pleased to be an early supporter of the GSMA Device Connection Efficiency guidelines through the support for the RPM (Radio Policy Manager) feature. RPM is supported across the Qualcomm Technologies, Inc. family of LTE chipsets from the entry level 200 series all the way up to our top of the line 800 products."

Brent Formigli, Senior Director of Business Development, Qualcomm

"One of the challenges facing the Internet of Things is the possibility that a vast number of connected devices could overwhelm the data-carrying capacity of mobile networks."

Telenor Connexion, press release, January 2015

INTERACTION BETWEEN GSMA ONEM2M

THE FEATURES PROVIDED BY THE IOT CONNECTION EFFICIENCY GUIDELINES ARE BASED ON THE EXISTING 3GPP DEPLOYED NETWORK

FUTURE RELEASE OF 3GPP ALREADY PROVIDE SIMILAR SOLUTIONS

SOME OF THE FEATURE COULD BE GENERALISED FOR OTHER NETWORKS, THIS COULD BE IN THE SCOPE OF THE NEWLY CREATED ONEM2M WORK ITEM “EFFICIENT COMMUNICATIONS” IN ORDER TO PROVIDE AN HARMONISED APPROACH ACROSS DIFFERENT TECHNOLOGIES.

GSMA WOULD LIKE TO RECEIVES UPDATES ABOUT THE PROGRESS OF THE NEW WORK ITEM

Connected Living

IoT SECURITY

CONNECTED LIVING - IOT SECURITY WORK

WHY FOCUSING ON SECURITY?

A result of a survey of 1000 enterprises discovered that 77% said they wanted to develop IoT services and the biggest concern was security/privacy.

There are an increasing report of incidents on the media.

SECURITY MUST EXIST BECAUSE:

Protect Personal Data

Guard against fraud

Protect the vulnerable

And for many other well documented reasons……

CONNECTED LIVING - IOT SECURITY WORK

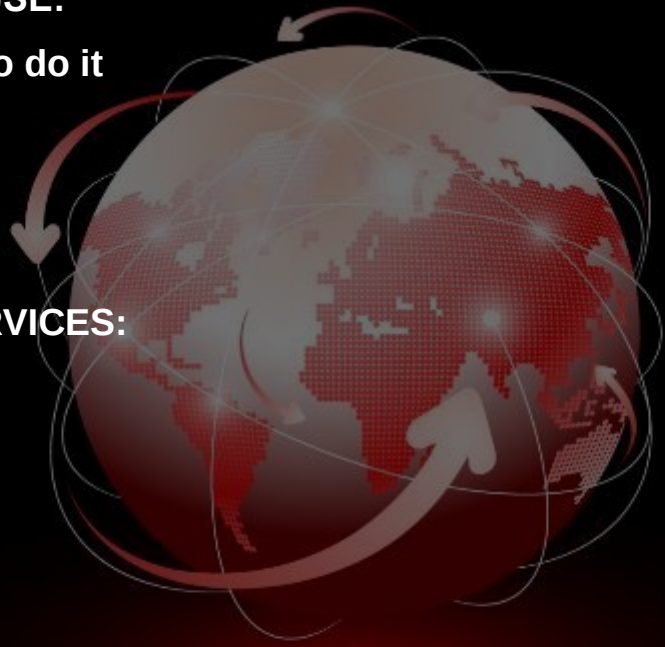
SECURITY IS A NECESSARY EVIL, IT IS SOMETHING THAT YOU DO NOT LIKE BUT WHICH MUST EXIST OR HAPPEN.

GENERALLY WE DON'T LIKE SECURITY BECAUSE:

- **It restricts what I want ot do and how I want to do it**
- **It can be complicated and time consuming**
- **It can be costly**

CONSEQUENCES OF INSURE END-TO-END SERVICES:

- **Brand and Trust impact**
- **Legal and regulatory consequences**
- **Possible high repair cost**



GSMA IoT SECURITY - EXISTING ACTIVITY

GSMA Fraud and Security Group

- Permanent working group within the GSMA
- Focus on all aspects of Networks, Devices, Applications and SIM

GSMA Connected Living Programme

- CLP.04 “End-to-End Security for M2M & IoT” Position paper
- CLP.06 “End-to-End Security for M2M & IoT” Whitepaper
- Both papers are available in InfoCentre for all GSMA members

GSMA IoT SECURITY - EXISTING WHITEPAPER

It is designed to help the mobile industry to establish a common understanding of IoT related security issues.

As security is often dependent on the weakest link, all stakeholders need to be committed to a commonly-agreed security baseline.

The whitepaper:

- is a result of interviews with experts, companies and organisations deploying IoT services.
- Contains analysis of use cases – Automotive, Smart Home, Health, Smart Cities
- Includes challenges - Low power, Low cost, Low processing capability.
- It provides recommendations to further develop:
  - Security education
  - Incident response and disclosure
  - Industry position on data protection and data sovereigntySecurity standards for products, processes and people
  - Software update handling
  - End-point security for IoT devices
  - Security audit mechanisms

GSMA IoT SECURITY - NEXT STEP

FOCUS FOR 2015/2016

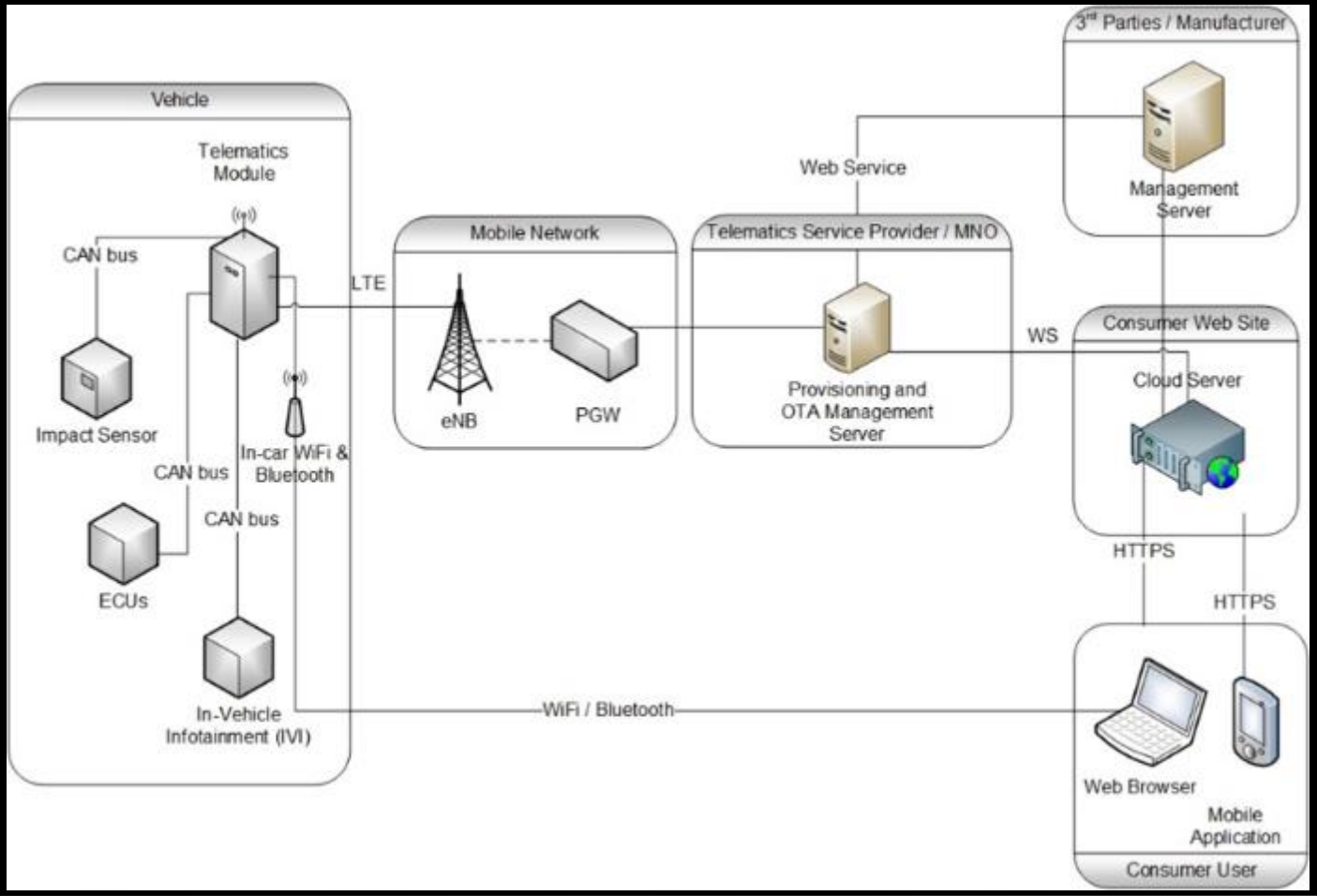
- Building upon the recommendations contained in our “End-to-End Security for M2M & IoT” Whitepaper the GSMA will now develop a set of IoT Security Guidelines

GUIDING PRINCIPLES:

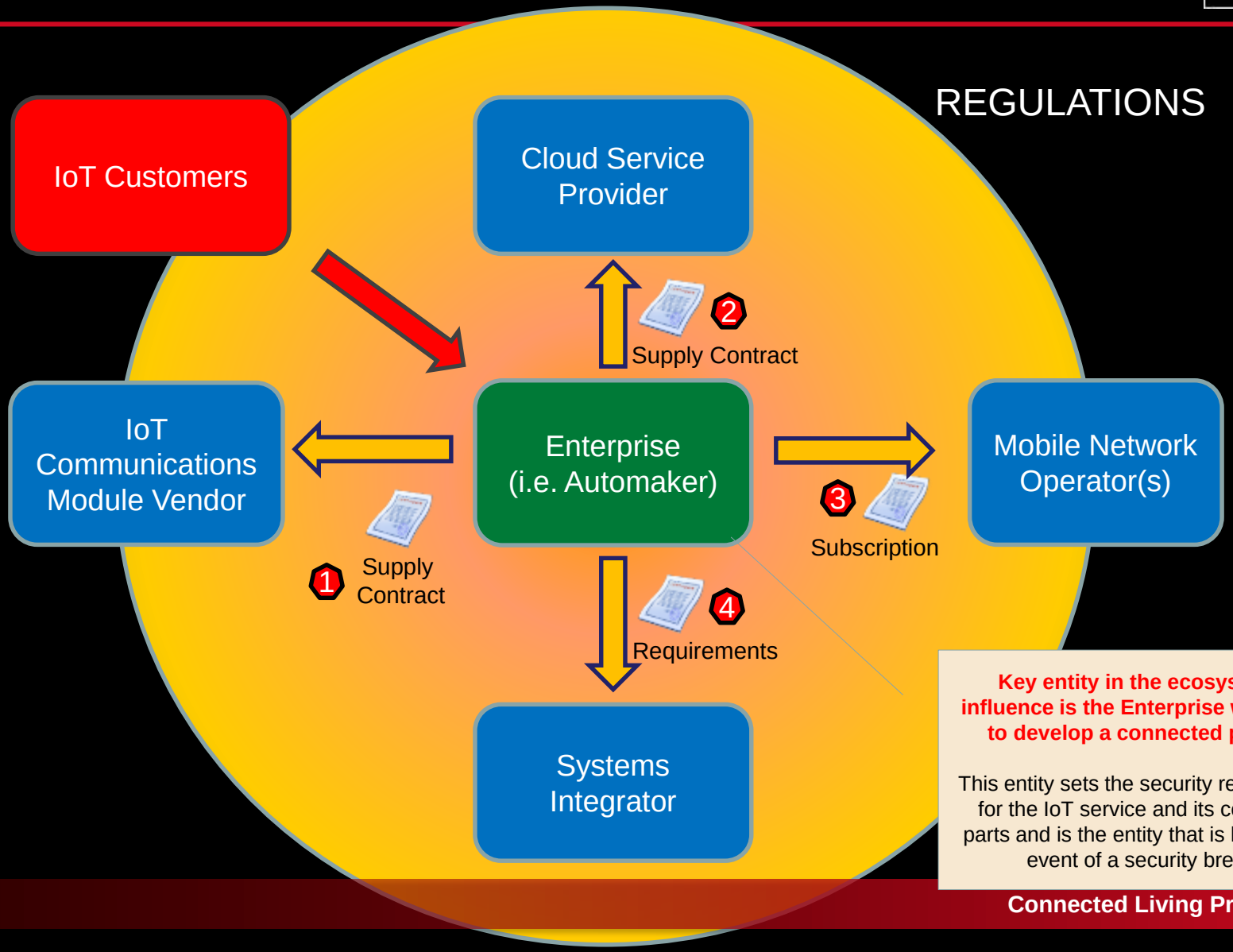
- Must be relevant to the whole IoT ecosystem – not just mobile network operator centric.
- Focus on the ‘here and now’ - using existing standardised technology, methods and procedures where possible.
- Cover Security aspects related to Identity, Confidentiality, Integrity and Availablity/Reliability.
- Must be industry agnostic

GSMA IoT SECURITY - ECOSYSTEM RELATIONSHIPS

Multiple suppliers, multiple developers, multiple bits of hardware!



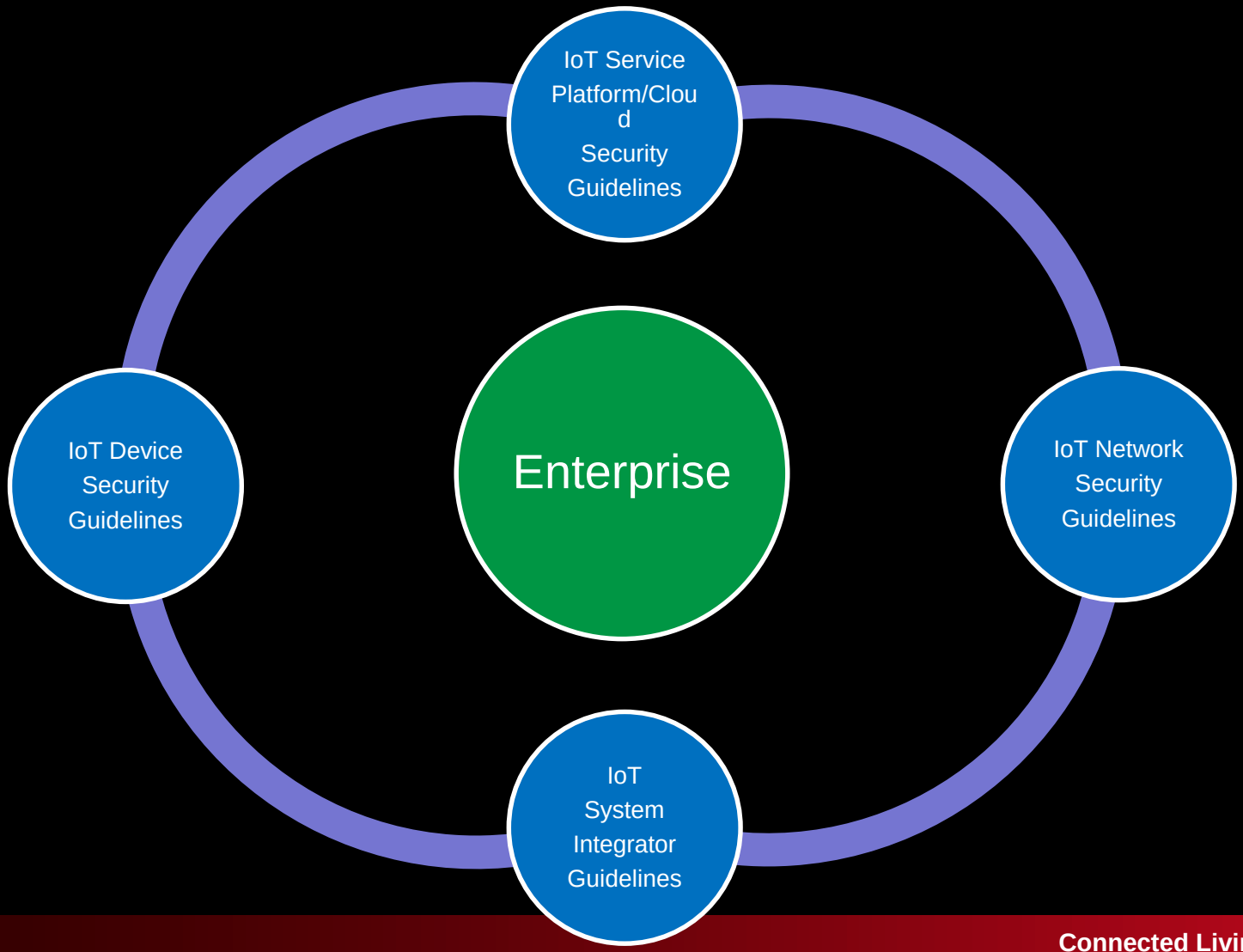
GSMA IoT SECURITY - IOT ECOSYSTEM



Key entity in the ecosystem to influence is the Enterprise who wants to develop a connected product.

This entity sets the security requirements for the IoT service and its constituent parts and is the entity that is labile in the event of a security breach.

GSMA IoT SECURITY - PROPOSED APPROACH



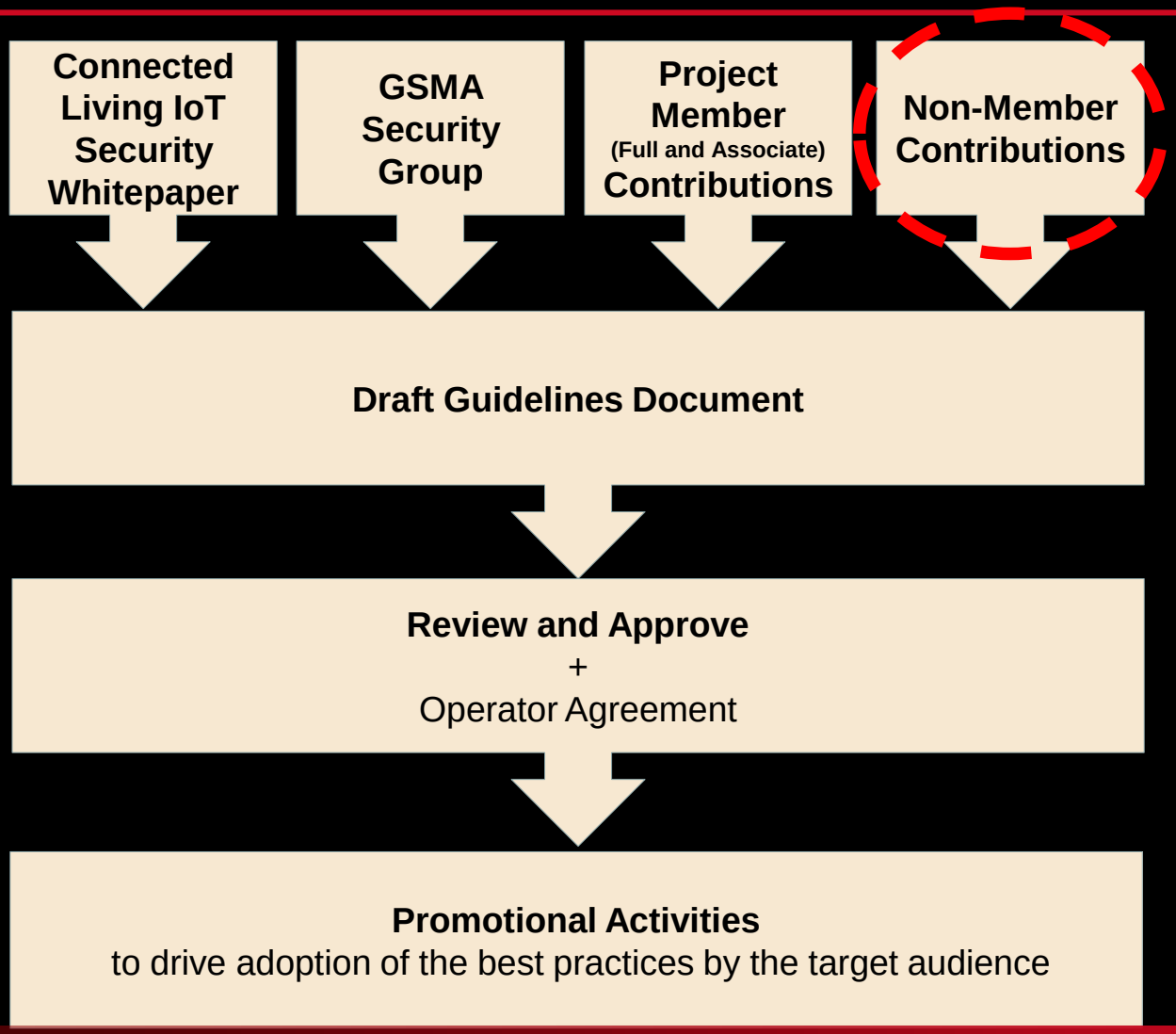
IOT SECURITY PROJECT - DELIVERY PROCESS

1. Review and reuse all relevant existing IoT Security material.

2. Merge into 1st draft document for review and development

3. Review and approve at working group level. Followed by approval.

4. Drive adoption via Special Interest Groups (SIGs) and promotion at industry events (MWC)



INTERACTION BETWEEN GSMA ONEM2M

GSMA IS INTERESTED TO UNDERSTAND THE SYNERGIES BETWEEN ONEM2M SECURITY FRAMEWORK AND OTHER EXISTING DEPLOYED FRAMEWORK.

GSMA IS WELCOME MEMBERS THAT WOULD LIKE TO CONTRIBUTE TO THE GUIDELINES.

COMMENTS AND QUESTIONS

ECOSYSTEM ENGAGEMENT

THE GSMA WORKS CLOSELY WITH ITS PARTNERS IN THE ECOSYSTEM TO ALIGN IT'S STRATEGY, UNDERSTAND THEIR REQUIREMENTS AND ENSURE ITS INITIATIVES ARE ADOPTED. BY DETERMINING COMMON CAPABILITIES WE WILL MAKE A POSITIVE IMPACT ON THE INDUSTRY CREATING SOLID FOUNDATIONS FOR M2M AND ENABLING IT TO GROW.

KEY ECOSYSTEMS INCLUDE

AUTOMOTIVE	HEALTH	LEARNING	UTILITIES	TRANSPORTATION
				

MORE INFORMATION

To find out more about the GSMA Connected Living programme visit our website at www.GSMA.com/connectedliving

Email us at ConnectedLiving@gsma.com