SECMP0037 ‘Pairing Local PPMIDs’ and SECMP0038 ‘Sending Commands via PPMIDs’

26th February 2019

Gemserv

SECMP0037 ‘Pairing Local PPMIDs’ - Overview

- SECMP0037 was raised to remove the 60-minute limit in place on a Communications Hub to allow a Prepayment Metering Interface Device to be connected locally without requiring a reliable Wide Area Network connection or engineer intervention.

- Following the last Working Group in August 2017 it was decided that the security implications and costs of implementing this modification needed to be established. Aspects of the modification were included in the annual SSC risk assessment.

- This risk assessment has been reviewed by the SSC and another iteration was requested with more detail on the Inter-PAN.

SECMP0037 ‘Pairing Local PPMIDs’- Proposed Solution

- The solution proposed meant removing the 60-minute window during Communication Hub power up to allow for devices to be connected at any time.

- Suppliers could then post a replacement device to a customer and be able to connect it locally via the PPMID acting as a HHT. The PPMID will connect to the Communication Hub via the ZigBee Inter-PAN. The proposed solution requires extending the local pairing mechanism that is already included in the Technical Specifications.

SSC risk assessment summary for SECMP0037

- *"The Communications Hub inter-PAN link is used to establish a link key between a Hand Held Terminal (HHT) and a Communications Hub through Certificate Based Key Exchange (CBKE). However, the SSC risk assessment confirms that security controls such as a 60 minute time-out following Power-up are needed to mitigate and reduce the availability risks that arise from an attack within local radio range of a Communications Hub, particularly in areas of high population density.*

- *This risk increases as a result of Dual Band Communications Hubs that use 868Mhz frequency and widen the area of radio range and will increase further as a result of Alt HAN design proposals. The extent of these risks and any further necessary mitigations continue to be assessed".*

Discussion points

- **Why was the 60-minute time out introduced?**
- The limit was originally introduced to limit the period in which malformed messages could be submitted via Inter-PAN. The reasons for this however are not fully understood.
- **What are the risks associated with removing the 60 minute time-out?**
- SSC have stated that they are looking more widely at Consumer Access Devices in general and the potential risks they pose.
- **What sections of the SEC would need amending to implement SECMP0037?**
- Initially the IMR stated that that GBCS section/clause 10.5 would need to be removed and;
- The CPA Security Characteristics for a Communication Hub would also need amending via BEIS or the SSC.

Potential Changes to CPA

CPA Security Characteristics

Smart Metering – Communications Hub

DEV.1.1.M949: Secure Inter-PAN connection.

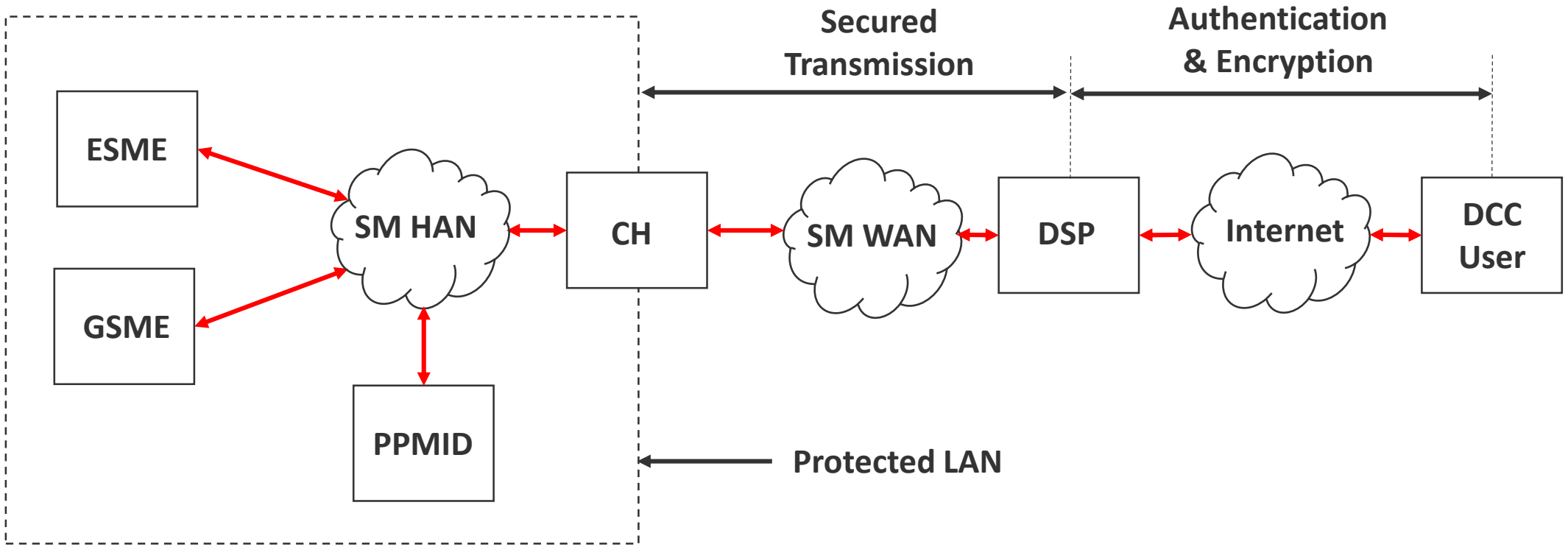
This mitigation is required to counter sending commands on an unauthorised Inter-PAN connection.

At Foundation Grade the product is required to only enable ZigBee Inter-PAN temporarily on power-up and only allow authorised connections. The communications hub shall only enable Inter-PAN joining after power-up for a short period, defined in [e, 4.4.7], to enable an authorised HHT to establish a secure connection as specified in [d, 10.5] for installation or maintenance.

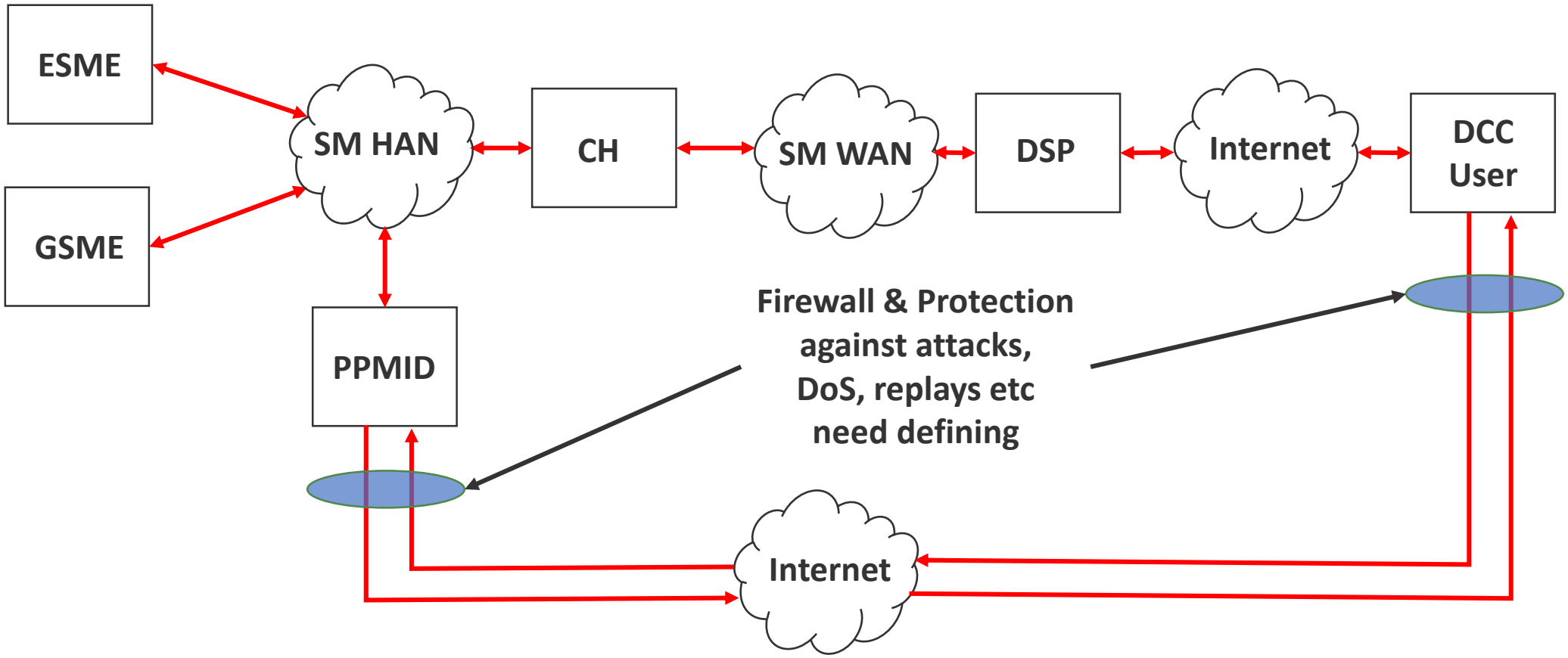
SECMP0038 ‘Sending Commands via PPMID’ - Overview

- Should a SMETS 2 device be installed in an area that experiences intermittent or no-WAN then there can be instances in which it is difficult to deliver configuration Commands in a sufficiently timely manner. This is an issue as prepayment customers living in these areas may find themselves without a supply of energy to their homes and there is no current SMETS2 solution developed to deal with this issue, unlike in SMETS1, other than sending an engineer with a HHT to the premise.
- The proposed solution is to extend the range of mechanisms used to deliver Commands to the CH in Consumers’ premises. This will include via an ‘enhanced PPMID’.
- The CH will need to be able to deliver and receive Commands to the target Device. This range of delivery mechanisms will allow Commands to be delivered when there are issues with the Communication Service Provider’s (CSP) Wide Area Network (WAN) connection to the CH.

Standard Communication Smart Meter System



Communication via PPMID

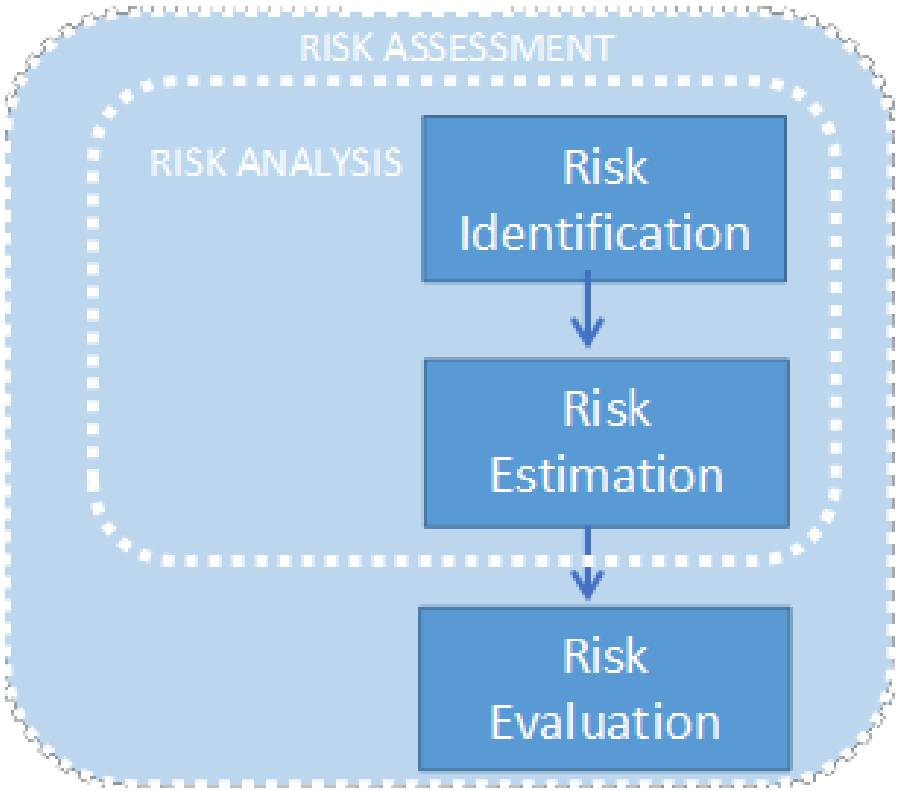


SECMP0038 - Risk Assessment

Presentation of Results

Risk Assessment Methodology

- Aligned with **ISO27005**



- Identifying assets that require protection (hardware, software)
- Identifying relevant threats and vulnerabilities (application based, physical)
- Identifying exploitable vulnerabilities within the proposed architecture
- Determining the impacts
- Estimating the level of risks posed by threat agents

Risk Scoring System

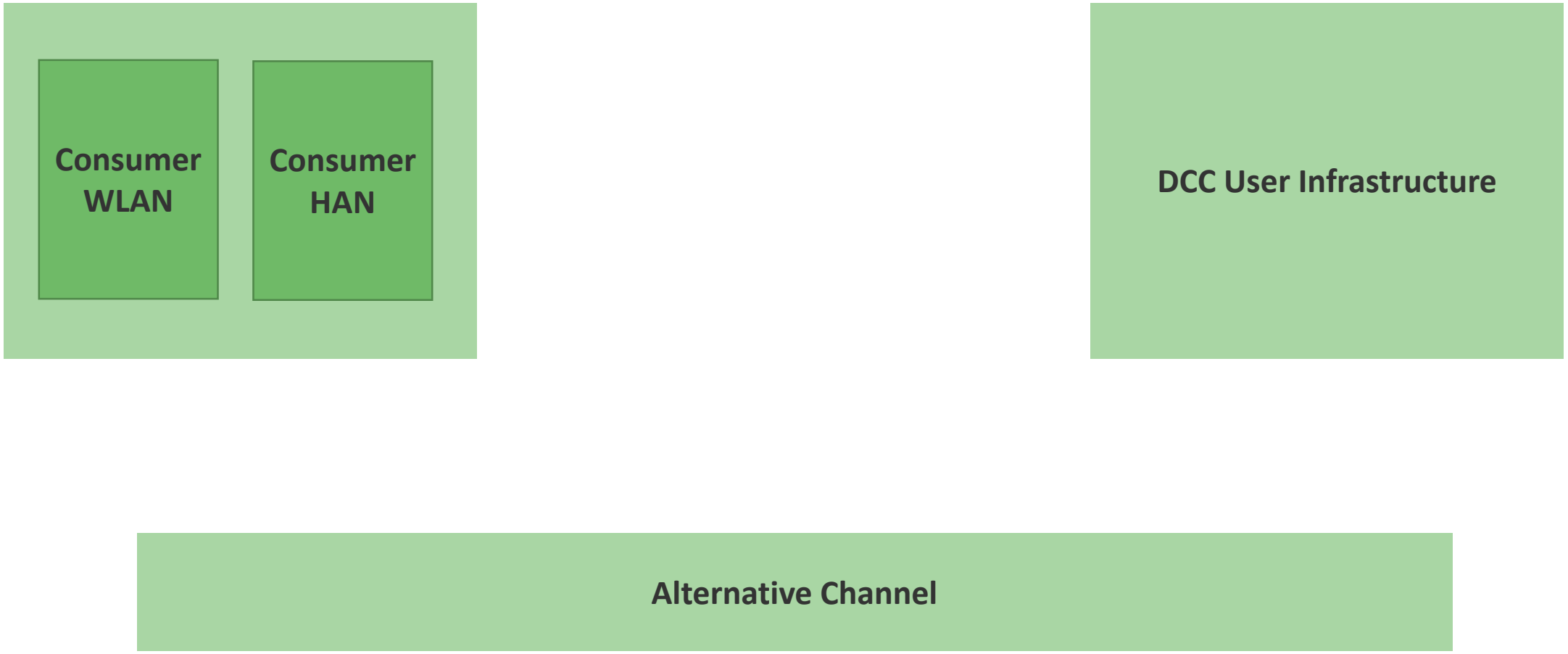
- **Likelihood**: possibility of an event occurring one time, and on the reoccurrence of such event.
- **Threat**: actor's capability score multiplied by actor's motivation score.
- **Impact**: maximum score among Confidentiality, Integrity, Availability (CIA) rating.

- Formula for overall score: **(Likelihood + Threat) x Impact**

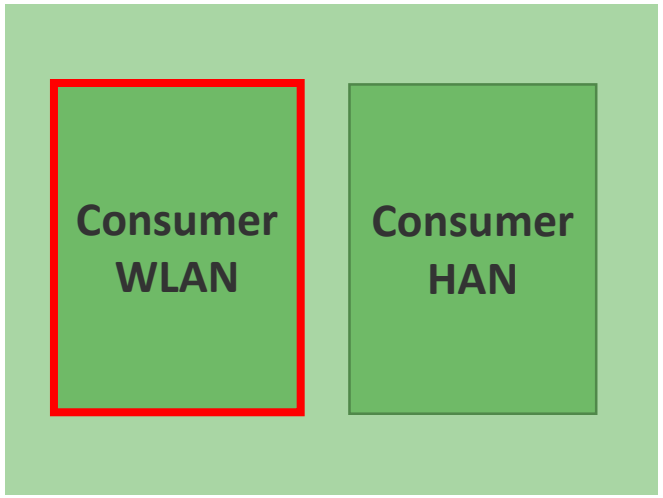
Identified Risks per Deliverable

Deliverable	Total Number of Risks Identified	Critical Risks	High Risks	Moderate Risks	Low Risks	Negligible Risks
Deliverable 1	30	0	6	8	16	0
Deliverable 2	23	0	6	8	9	0
Deliverable 3	34	0	7	8	18	1
Deliverable 4	11	0	3	4	4	0
Total	98	0	22	28	47	1
Unique Risks	**46**	**0**	**8**	**13**	**24**	**1**

Risk Areas

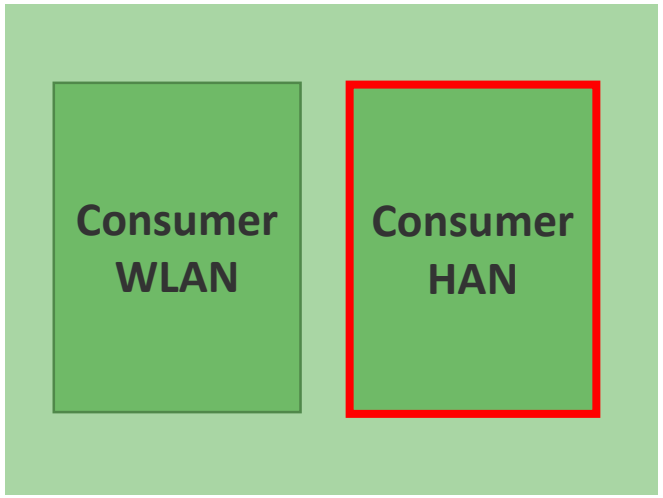

Consumer WLAN
Consumer HAN
DCC User Infrastructure
Alternative Channel

Risk Categories – Consumer WLAN



- **Reliability**
  - No QoS on bandwidth guaranteed
  - Incorrect Configuration
  - Consumer Equipment Ownership
- **Security**
  - No security assurance, i.e. open to wireless sniffing
  - Risk of Infection from other Wi-Fi devices
  - Patching, firewall, malware requirements
  - Extending attack surfaces to the internet

Risk Categories – Consumer HAN



- **Reliability**
  - No assurance on PPMID availability
  - Incorrect Configuration
- **Security**
  - No security assurance
  - Integrity verification of messages
  - Physical tampering

Risk Categories – DCC User Infrastructure

DCC User Infrastructure

- **Reliability**
  - No assurance on HES
  - Incorrect Configuration
  - Asset Register Updates
  - Management Overhead – Cost and Effort
- **Security**
  - Security Assurance on Systems and Processes

Risk Categories – Alternative Channel

Alternative Channel

- **Reliability**
  - Management overhead – cost and effort
  - Channel availability
- **Security**
  - No security assurance – node to node communication
  - Verification Requirements

Overview of High Risks

Excel Sheet – Risk Register

High Level Recommendations

- **PPMID** – Technical and Security Assurance
- **HES SYSTEMS** – Technical and Security Assurance
- **ALTERNATIVE CHANNEL** – Transport Security
- **SEC and SUPPLIERS** – Policies and Operational Procedures (Change of Supplier Scenario)
- **CONSUMER** – Awareness and Data Privacy Impacts on Consumer Local Area Network (LAN)

Next Steps

- **SECMP0037 ‘Pairing Local PPMIDs’**
- The Working Group are asked to consider the following:
  - the Legal Text requirements
  - the Business Requirements
  - to request Preliminary Assessment

- **SECMP0038 ‘Sending Commands via PPMIDs’**
- The Working Group are asked to consider whether they should proceed to Working Group Consultation

Thank you

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 0039

LLOYD'S REGISTER · LRQA ISO 9001 001

CYBER ESSENTIALS PLUS