OpenADR via the UK Smart Meter System

Nick Winfield

L+G IDSR Project Steam 1 and Stream 2

- IDSR (Interoperable Demand Side Response) Stream 1 and Stream 2 projects sponsored by Department for Energy Security & Net Zero*
  - Stream 1 is IDSR via the internet
  - Stream 2 is IDSR via the SM(Smart Meter) System
    - There are 2 different routes for stream 2
      - 2a Security and communication via the SM system
      - 2b Security via the SM system and communication via the internet
  - Landis+Gyr are involved in both Stream 1 and Stream 2 projects

** The IDSR programme is part of the up to £65m Flexibility Innovation Programme within the Department for Energy Security and Net Zero's £1 billion Net Zero Innovation Portfolio.*

PAS1878

- Energy smart appliances – System functionality and architecture
- Purpose – To enable standardized control of energy smart appliances (ESAs), subject to explicit consumer consent
- OpenADR is the primary controlling protocol

PAS 1878:2021

Energy smart appliances – System functionality and architecture – Specification

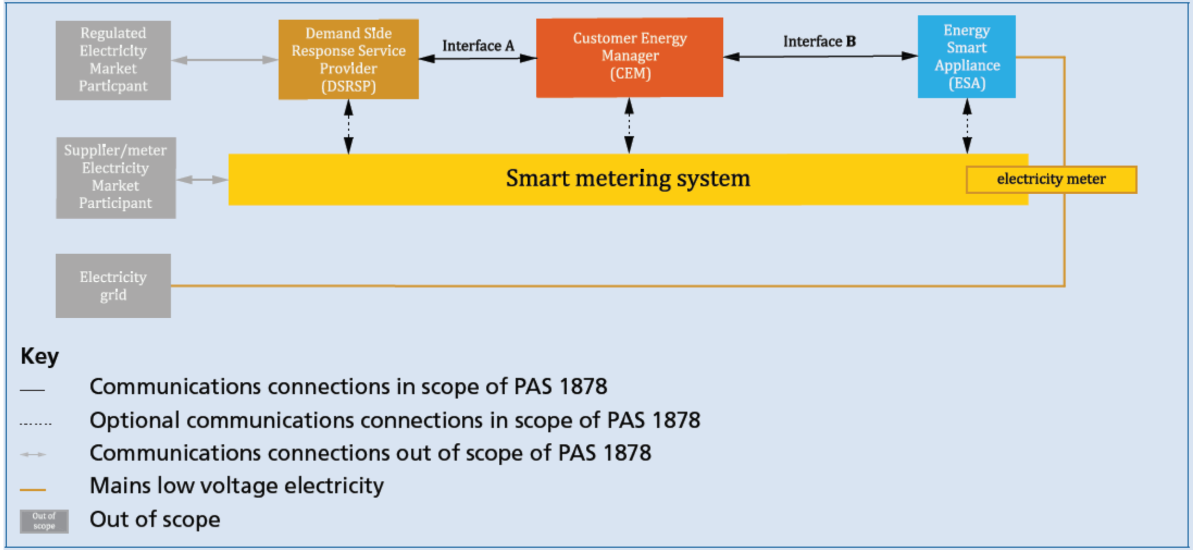
Licensed copy. Version correct as of 26/01/2022 © British Standards Institution

Department for Business, Energy & Industrial Strategy

bsi.

PAS1878

Logical DSR architecture and communications



Regulated Electricity Market Particpant

Demand Side Response Service Provider (DSRSP)

Interface A

Customer Energy Manager (CEM)

Interface B

Energy Smart Appliance (ESA)

Supplier/meter Electricity Market Participant

Smart metering system

electricity meter

Electricity grid

Key

— Communications connections in scope of PAS 1878

······· Optional communications connections in scope of PAS 1878

←→ Communications connections out of scope of PAS 1878

— Mains low voltage electricity

Out of scope Out of scope

Interface A – OpenADR

Interface B – Manufacturer specific

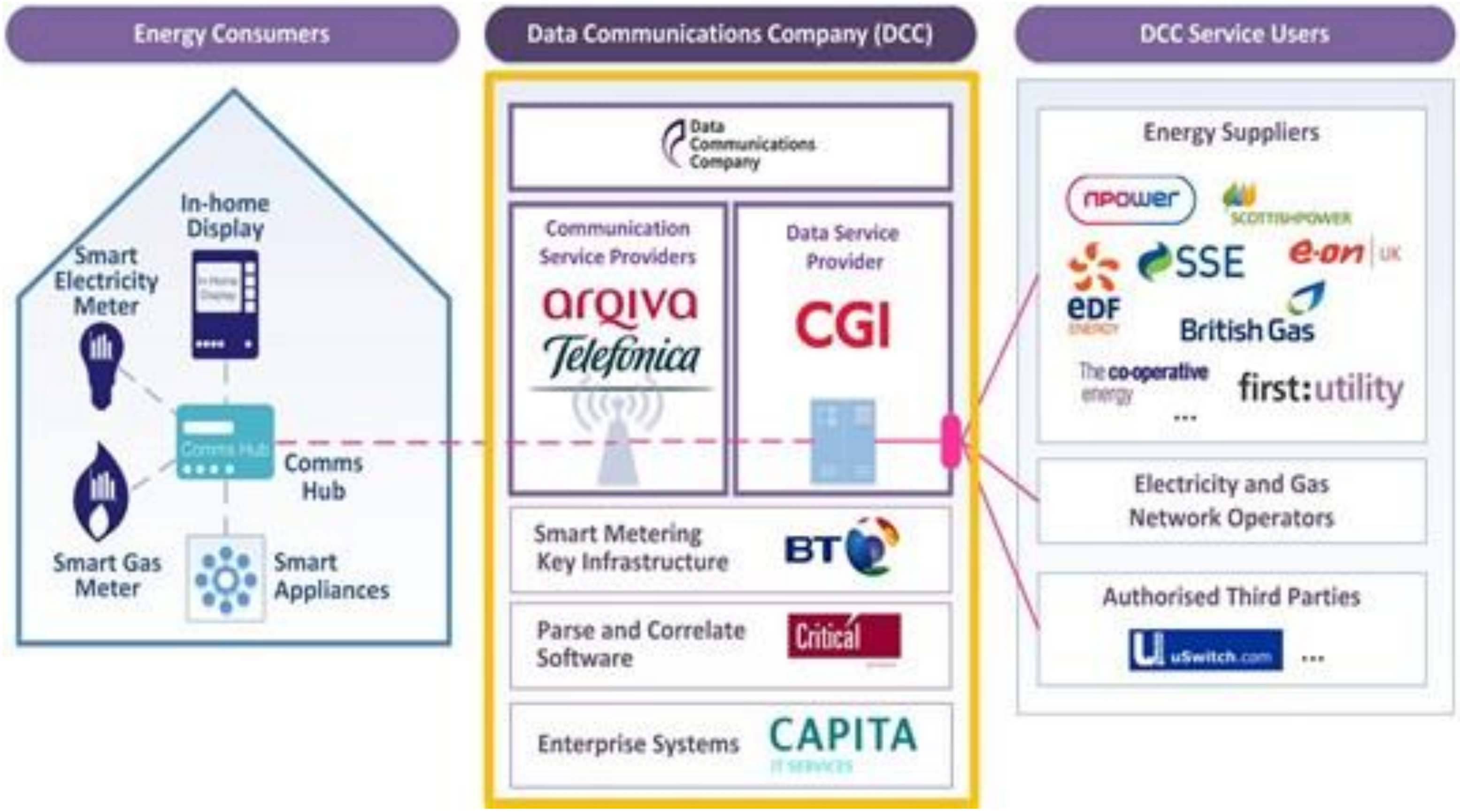
Stream 2 – Smart meter system

- Communication and security handled by the SMETS2 Smart Metering System
  - The project will demonstrate OpenADR communications using the smart meter Certificate authority
  - Communications will be demonstrated using both the smart meter system and via a hybrid internet/SM route

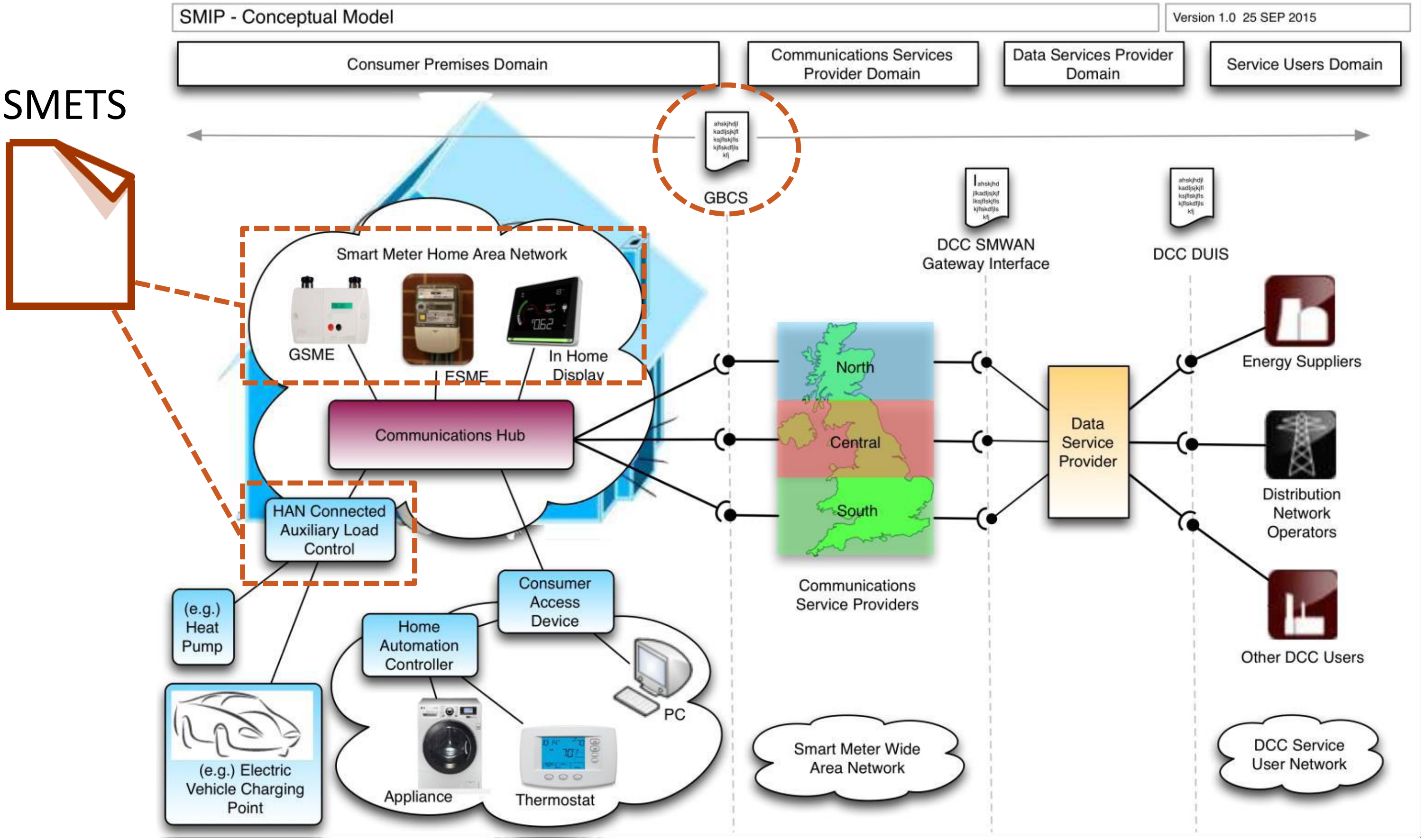
UK Smart Meter System

- SMETS = Smart Metering Equipment Technical Specifications
- SMETS2 meters were introduced in 2018/19 to resolve the interoperability issues with SMETS1 meters.
- From 2019 onwards only SMETS2 meters installed. L+G have supplied SMETS2 meters since the start
- SECAS (Smart Energy Code Administrator and Secretariat) provide governance of the scheme

SMETS2 Smart Meter System



SMETS2 Smart Meter System


SMETS
SMIP - Conceptual Model
Version 1.0 25 SEP 2015
Consumer Premises Domain
Communications Services Provider Domain
Data Services Provider Domain
Service Users Domain
GBCS
DCC SMWAN Gateway Interface
DCC DUIS
Smart Meter Home Area Network
GSME
ESME
In Home Display
Communications Hub
HAN Connected Auxiliary Load Control
(e.g.) Heat Pump
(e.g.) Electric Vehicle Charging Point
Consumer Access Device
Home Automation Controller
Appliance
Thermostat
PC
North
Central
South
Communications Service Providers
Data Service Provider
Energy Suppliers
Distribution Network Operators
Other DCC Users
Smart Meter Wide Area Network
DCC Service User Network

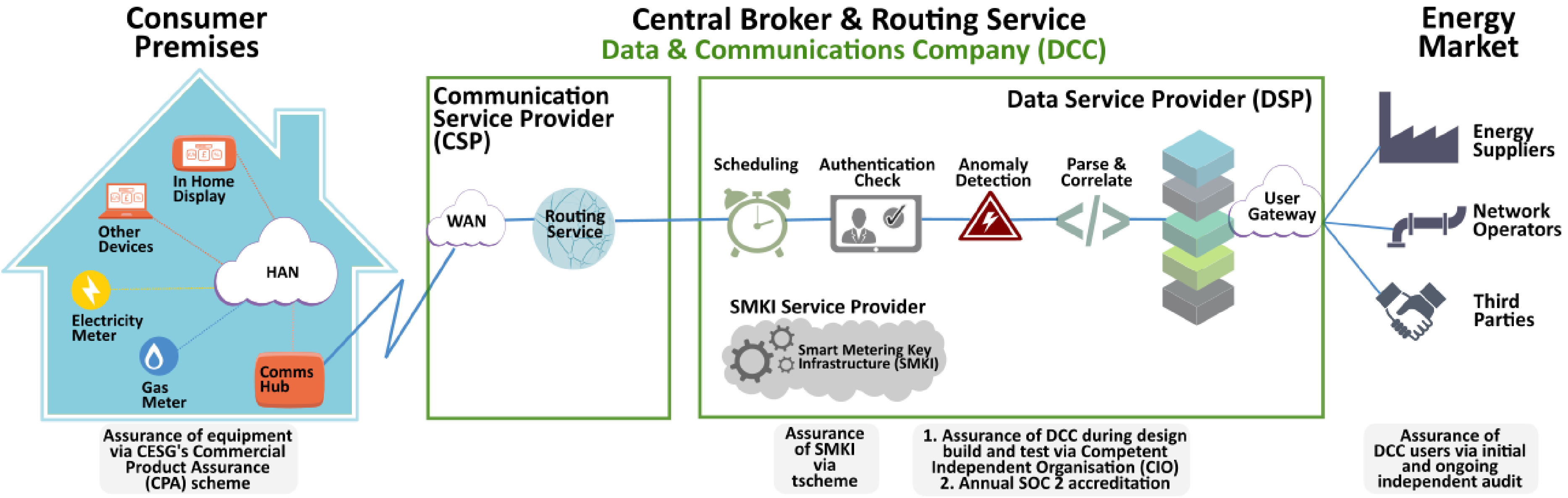
Why Use the SM System

- The SMETS2 communication system has already been set up to communicate with and collect data from >50M smart meters in the UK
  - The necessary infrastructure is already in place
  - Highly regulated
  - It is a highly secure network with a single certificate authority (SMKI)
  - Private network

SMKI

- SMKI is the Smart Meter Key Infrastructure
  - Provides the single certification authority for the smart meter system
  - Closed system, set up specifically for smart meter system
    - More secure than open internet systems
  - Government controlled and overseen by NCSC

Security advantages of the SM system



Assurance of equipment via CESG's Commercial Product Assurance (CPA) scheme

Assurance of SMKI via tscheme

1. Assurance of DCC during design build and test via Competent Independent Organisation (CIO)
2. Annual SOC 2 accreditation

Assurance of DCC users via initial and ongoing independent audit

- Authentication Check – Validate certificates
- Anomaly Detection - Check for unusual patterns
- Parse & Correlate – Check the message is correctly constructed

Challenges of using the SM system

- All smart devices on the Smart Meter network need to be CPA approved. This is a difficult and slow process, and not suited to non ‘standard’ device types. And not suited to rapid product release.

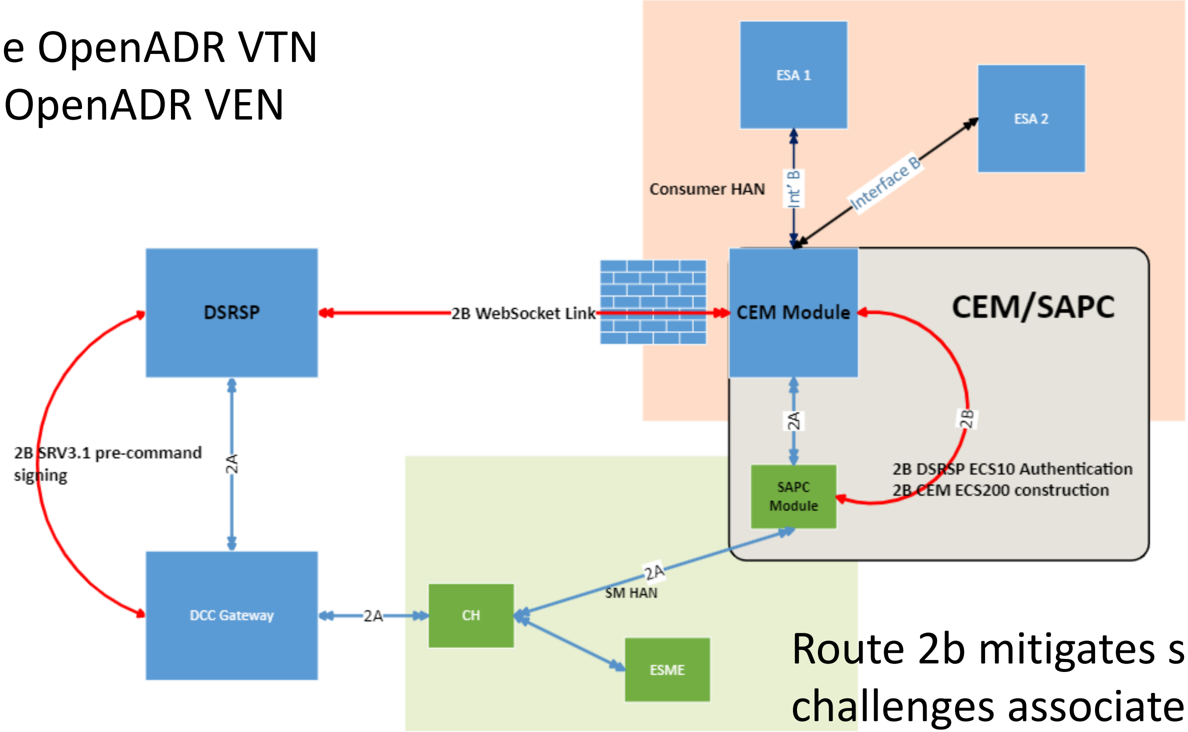
- The SMETS2 system does not currently cater for the transmission of OpenADR data
  - It is necessary to ‘re-purpose’ existing SMETS2 features
    - May cause issues with the above CPA approval

- Latencies in the system are likely to be higher than if using direct IP connection
  - OpenADR messages will be quite large compared to most SM messages, and will be split into many fragments

- The capacity of the system has not been proven for the potentially many millions of additional connections, and related additional bandwidth required.

Elements of our IDSR solution

The DSRSP is the OpenADR VTN
The CEM is the OpenADR VEN



Interface A via:

- 2A: DCC Tunnelling Protocol
- 2B: Tunnelling Protocol Alternate Route

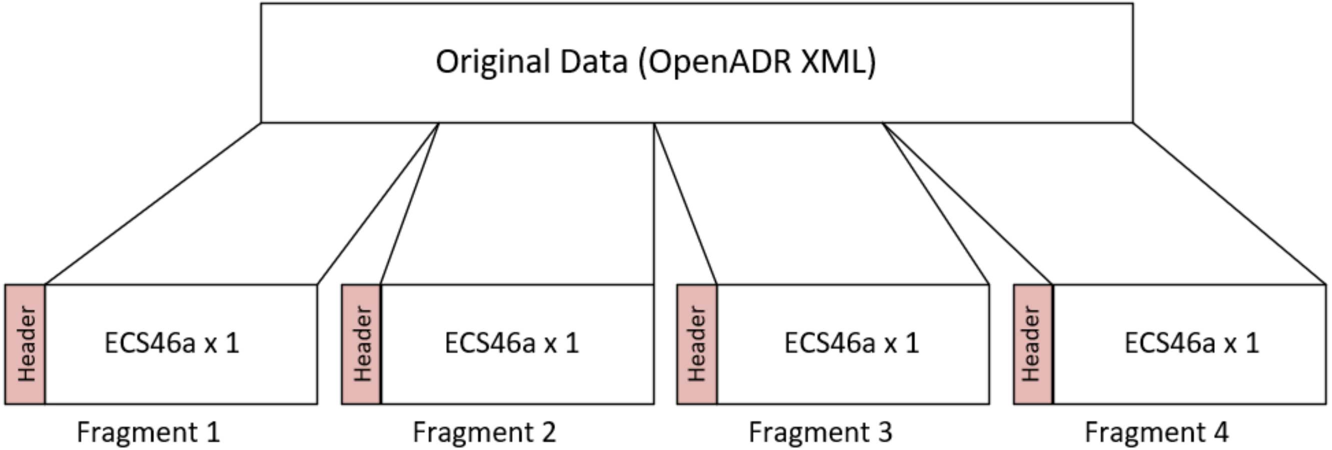
Route 2b mitigates some of the challenges associated with the SM system

OpenADR via the Smart Meter System

- Tunnelling
  - ECS46a (UpdateDeviceConfiguration(AuxiliaryLoadControlDescription)) will be used to send OpenADR to the ESAs
    - ECS46a is normally used to label Load Controllers
    - The usable payload of ECS46a is only 110 octets
    - Smart meter system signed OpenADR text will be fragmented into as many ECS46a payloads as necessary
    - Sequencing info will be included to avoid ‘out of order’ fragments causing a problem
    - Open ADR XML will be reconstructed by the CEM

  - ECS200 (Operational Update) will be used to send OpenADR text to the DSRSP
    - The usable payload of ECS200 (Operational Update) is 1,062 octets
    - Fragmentation similar to above will be used.

OpenADR via the Smart Meter System



Header = 3 octets	Bits	
Control bits	5	Originator, Compression Encoding +
Fragment index	11	Fragment number 0-2047
Message ID	8	Used to group fragments

Data is Compressed using Zlib compression, and uses Base64 Encoding as payload is for printable characters only

What about the OpenADR Security

- We will **not** be using the mutual http client authentication and XML signatures as defined in IEC62746-10-1
  - Only OpenADR unsigned payload will be sent via the SM route
    - OpenADR https/xmpp end points not used
  - Security will be provided by the SM System
    - Anomaly detection
    - Private smart metering key infrastructure (SMKI)
      - Single authentication authority
    - Message signing mechanisms, as used for handheld terminals – used for route 2B communication
    - For route 2b Websocket provides a secure link using TLS, this is configured using the 2a route

What do we expect to learn from Stream 2

- Practical experience of using the SM system to implement IDSR according to PAS1878
- Test how the solution passes through CPA approval
- An understanding of how latencies in the system might affect IDSR performance
- Suggest how SMETS may be enhanced in future with tunnelling specific GBCS commands.
- Comparison between Stream 1 (OpenADR via internet) and Stream 2 (OpenADR via smart meter system)
- Comparison between the 2 proposed routes for Stream 2 (2a and 2b)

Thank you for your attention

Nick Winfield
Product Manager

Nick.Winfield@landisgyr.com

Landis+Gyr Ltd
www.landisgyr.com/europe