



NETWORKS

SMART AMI HES AND METER PROCUREMENT SOLUTION OVERVIEW



0. Document History

Ver	Details of Changes	By	Date	Reviewed by
0.1	Initial Reversion of Solution Overview from previous procurement considering approved outcomes of Meter+ Decision notes.	All	16/02/2025	BOI Meter+ Team

0.1 Contributors

Name	Role
Gerry McGarry	Convenor / Project Lead
Pat Cooney	Core Meter+ Procurement
Mike Buss	Meter Specialist
Patrick O'Donovan	Project Manager / Business Analyst
Edward Mace	HES Specialist
Cliff Nyangau / Frank De Azevedo	Security Architect

0.2 Document Approval

Name	Role	Signature	Date
Gerry Mc Garry	Project Lead	GMCG	12/03/2026

Table of Contents

0. Document History	2
0.1 Contributors	2
0.2 Document Approval	2
1. Introduction	10
1.1 Scope of this Procurement	10
1.2 Historical Smart Metering Programme Scope	11
2. CRU Smart Metering Programme (2019 – 2025)	12
2.1 Phase 1 Summary	12
2.2 Phase 2 Summary	12
2.3 Phase 3 Summary	13
3. ESB Networks Implementation Overview	14
3.1 Introduction	14
3.2 ESB Project Model	15
3.2.1 <i>Concept Phase</i>	15
3.2.2 <i>Definition phase</i>	15
3.2.3 <i>Preparation Phase</i>	16
3.2.4 <i>Execution Phase</i>	16
3.2.5 <i>Transition Phase</i>	16
3.2.6 <i>Knowledge Phase</i>	16
3.2.7 <i>High Level Plan</i>	16
3.3 Scope of Meter+ Functionality Releases	17
3.3.1 <i>Meter+ Release 1 Scope</i>	17
3.3.2 <i>Meter+ Release 2 Scope</i>	18

3.3.3	<i>Meter+ Release 3 (and further releases) Scope</i>	18
3.4	Execution Phase	19
3.4.1	<i>Meter+ Design Overview</i>	19
3.4.2	<i>Meter+ Build Overview</i>	19
3.4.3	<i>Meter+ Testing Overview</i>	21
3.5	Transition Phase	22
3.5.1	<i>Operation Life</i>	22
4.	High Level Advanced Metering Infrastructure (AMI) Capabilities and Scope Features	25
4.1	High Level Capabilities	25
4.2	High Level Scope Features	26
4.2.1	<i>General</i>	26
4.2.2	<i>Tariffs</i>	26
4.2.3	<i>Estate / Device Management</i>	27
4.2.4	<i>Local Data connections</i>	27
4.2.5	<i>Instrumentation and Smart Network Management</i>	29
4.2.6	<i>Firmware (FW) and Configuration Management.</i>	30
4.2.7	<i>Security Management</i>	37
4.2.8	<i>ESB Smart Metering Companion Specification</i>	42
5.	Smart Electricity Meters (SEM)	43
5.1	General	43
5.2	Basic meter construction and operation.	43
5.3	Communications	45
6.	HES Compatibility	47
6.1	Enhanced Meter Functions	47
6.1.1	<i>Security</i>	47
6.1.2	<i>Clock and Calendar</i>	47
6.1.3	<i>Tariffs</i>	47
6.1.4	<i>Thin prepayment</i>	48

6.1.5	<i>Power quality monitoring and control</i>	48
6.1.6	<i>Power Outage</i>	48
6.1.7	<i>Firmware update</i>	48
6.1.8	<i>Event Logging and alerts</i>	48
6.1.9	<i>Routine Data Transfer</i>	49
6.1.10	<i>Ad-hoc data transfer</i>	49
6.1.11	<i>Spare Capacity</i>	49
6.2	Integration of SEM into AMI ecosystem	49
7.	Head-End System Solution (HES)	50
7.1	HES High Level Scope	51
7.2	Key Features	53
7.2.1	<i>Security and Configuration by Design</i>	53
7.2.2	<i>Modular Structure, Operational Monitoring and Configuration</i>	53
7.2.3	<i>Transactional Data Store (TDS) and Reporting</i>	53
7.2.4	<i>Security Application</i>	53
7.2.5	<i>Credential receipt and management</i>	54
7.2.6	<i>Meter Messaging, Creation, routing and Validation</i>	54
7.2.7	<i>User Interface</i>	54
7.2.8	<i>Device State</i>	56
7.2.9	<i>Event Management</i>	56
7.2.10	<i>Device Configuration and Firmware / Configuration Campaign Management</i>	56
7.3	HES System Use Cases	56
7.3.1	<i>High Level Use Cases</i>	56
7.3.2	<i>Creation & Install, Removal and Swap out</i>	59
7.3.3	<i>Switch Operations</i>	59
7.3.4	<i>Meter Ping</i>	60
7.3.5	<i>Last Gasp (LG)</i>	60
7.3.6	<i>P1 Port</i>	60
7.4	HES System Interface Overview	60
7.5	HES High-Level Service Components	63
7.5.1	<i>Message Management Services</i>	64
7.5.2	<i>HES Security Services</i>	64
7.5.3	<i>Auditing</i>	65
7.5.4	<i>WAN Communication Gateway Services</i>	65
7.5.5	<i>Smart Device Management Services</i>	66
7.5.6	<i>Service Auditing and Reporting Services</i>	66

7.5.7	<i>System Monitoring and Management Services</i>	66
7.5.8	<i>Time Management</i>	66
7.5.9	<i>User Management Services</i>	67
7.5.10	<i>HES Campaign Management and Execution Services</i>	67
7.5.11	<i>Gateway Services</i>	67
7.5.12	<i>Data Management and Archiving Services</i>	67
7.6	KMS High-Level Service Components	68
7.6.1	<i>Gateway Services</i>	68
7.6.2	<i>Message Management Services</i>	68
7.6.3	<i>User and Access Management Services</i>	69
7.6.4	<i>Firmware and Configuration Storage and Retrieval Services</i>	69
7.6.5	<i>Service Auditing and Reporting Services</i>	69
7.6.6	<i>Time Management Service</i>	69
7.6.7	<i>Security Services</i>	69
8.	Non-Functional Requirements Overview	71
8.1	Security	71
8.1.1	<i>Message Security</i>	71
8.1.2	<i>SEM Use Case Security</i>	71
8.1.3	<i>Gateway Security</i>	71
8.1.4	<i>KMS Security</i>	72
8.1.5	<i>Data Security</i>	72
8.2	Service Availability and Disaster Recovery	72
8.2.1	<i>Data integrity and Backup</i>	72
8.3	Performance and scalability	73
8.3.1	<i>Infrastructure Requirements</i>	73
8.3.2	<i>Design Flexibility</i>	73
8.3.3	<i>Technologies used</i>	74
8.4	System Acceptance and ESB Environments	74
8.4.1	<i>System Acceptance</i>	74
8.4.2	<i>Feature Development and Acceptance</i>	74
8.4.3	<i>ESB and Supplier Environments</i>	74
8.5	Release Management	75
8.6	Software Releases and Maintenance	75



9. Home Area Network (HAN)	76
9.1 Overview	76
10. Integration and development of an Adaptor to the Siemens Energy IP/Gridscale Meter Data Management System (MDMS)	77
10.1 Overview	77
10.2 Meter Reading	78
10.3 Events	78
10.4 Provisioning	78
10.5 Switch Operations	78
10.6 On Demand Read / Meter Ping	79
10.7 Alerts and Last Gasp	79
10.8 P1 Port	79
10.9 Smart Device Configuration	80
10.10Firmware	80
10.11Summary of Performance	80
10.12Integration of the MDMS Adapter	80
11. Communications Service Provider (CSP)	81
11.1 CSP Scope	81
11.1.1 Communication service between ESB IT systems and SEMs	81
11.1.2 Communication configuration	81
11.1.3 Coverage and performance	81
11.1.4 Network improvement	82
11.1.5 Service reliability	82
11.1.6 Change of Communications Provider	82
11.1.7 Wireless mobile telecommunications technologies	82

12. Implementation Services	83
12.1 Meter+: Implementation scope for Release 1	83
12.2 Meter+: Implementation scope for release 2	84
12.3 HES Vendor Implementation Services	84
12.3.1 <i>Design of the HES System</i>	84
12.3.2 <i>Build of the HES System</i>	85
12.3.3 <i>Test of the HES System</i>	86
12.3.4 <i>SEM Delivery</i>	86
12.4 CSP Implementation Services	86
13. Enduring Support Services:	87
13.1 Common ITIL Services	87
13.1.1 <i>Incident management</i>	87
13.1.2 <i>Service Request management</i>	87
13.1.3 <i>Problem management</i>	87
13.1.4 <i>Change management</i>	87
13.1.5 <i>Contract and Service Review</i>	88
13.2 HES and SEM Vendor Enduring Support Services	88
13.2.1 <i>Support for Development of New Meter Firmware</i>	88
13.2.2 <i>Support for Development of New HES Features</i>	88
13.2.3 <i>Support for Development of New MDP/Companion Features</i>	88
13.3 Testing Services	89
13.3.1 <i>Support for test environments</i>	89
13.3.2 <i>Integration and testing resources</i>	89
13.3.3 <i>End device approval testing</i>	89
13.3.4 <i>Cyber Security Testing</i>	89
13.3.5 <i>SEM Delivery</i>	90
13.3.6 <i>Firmware issues</i>	90
13.3.7 <i>SEM, HES and Security Incidents</i>	90
13.3.8 <i>Troubleshooting</i>	90
13.3.9 <i>Documentation</i>	90
13.4 CSP Enduring Support Services	91



14. Glossary	92
15. Capability Descriptions (Selected)	101

1. Introduction

Please note the information contained in this document has been provided in good faith and is intended solely to assist Applicants in deciding to submit a Pre-Qualification Questionnaire (PQQ). The Contracting Entity provides no warranty as to the accuracy of the information which may unavoidably change at a later stage of the procurement process.

1.1 Scope of this Procurement

ESB Networks has been advancing its Smart Metering activities for several years. As part of the ongoing work to maintain and enhance the Smart Metering landscape, this procurement aims to implement a multi-vendor Head-End System (HES) together with Single-Phase and Three-Phase Whole Current and CT Smart Electricity Meters (SEMs), with full deployment and operational readiness required by the beginning of 2028. For the purposes of this procurement process and all associated documentation, this procurement of a Smart Advanced Metering Infrastructure (AMI) HES and meter will be referred to as Meter+.

The energy sector has experienced profound change in recent years, driven by rapid technological innovation, evolving regulatory frameworks, and shifting customer expectations. As a leading utility provider, ESB Networks remains committed to proactively adapting to these developments to ensure the continued delivery of reliable, efficient, and sustainable energy services. The procurement of the next-generation Advanced Metering Infrastructure (AMI) is a critical enabler in achieving these objectives and represents a key milestone in ESB Networks' long-term strategy for a modern, flexible, and customer centric electricity network.

It is envisaged that under the initial term of this contract ESNB will procure:

- Manufacture, supply, and delivery of up to 1.5 million Single-phase and Three-Phase Whole Current meters, as well as Single-Phase and Three-Phase CT meters, to be drawn down incrementally over the contract term, in line with ESB Networks' deployment requirements.
- Design (inclusive of Security Architecture), development, implementation, and integration of the required IT systems, including but not limited to the following:
 - A Head-End System (HES) capable of integrating with multiple SEM meter vendor's products concurrently, delivering high levels of interoperability across multiple devices, communications and system vendors within a complex AMI environment.
 - A Head-End System (HES) capable of meeting ESB Networks' functional, security, and performance requirement for 1.5 million SEMs initially and the capacity to scale up to potentially 3 million SEMs during the contract term.
 - The integration and development of an adaptor between the HES and the Siemens Energy IP Meter Data Management System (MDMS).
 - All associated integrations with existing ESB Networks systems and operational platforms.
 - Integration with Mobile Network Operator systems.

- Implementation of the AC Electricity Smart Meter Generic Companion Profile (ACE SM GCP) and local customisations to support the reliable and secure communication between the HES and SEMs across Wide Area Network (WAN) technologies.
- System implementation services, including configuration, testing, migration, and commissioning of the proposed IT systems.
- Ongoing support, maintenance, and management services to ensure continuity of operations, system performance, and long-term lifecycle management.

The context of the solution specification overview document is useful for potential respondents to understand the current operational landscape within which they are expected to deliver and maintain an operational solution within the existing Republic of Ireland (ROI) Smart meter Eco System.

1.2 Historical Smart Metering Programme Scope

ESB Networks DAC, as mandated by The Commission for the Regulation of Utilities (CRU), is responsible for the safe delivery of a platform that engages and enables the Irish electricity consumer and provides electricity suppliers with opportunities to improve their offerings to customers. The overarching objectives of the National Smart Metering Programme (NSMP) are:

- An educated engaged consumer.
- A shift in peak demand.
- Cost reduction - Smarter consumer usage within a dynamic pricing structure.
- Enhanced competitive retail market - provision of compelling retail products by Suppliers and accurate settlement and billing.
- Improved services from ESB Networks and Suppliers.
- Sustainable future.

More information on the programme as a whole can be found at [Smart meters and services | CRU.ie](https://www.cru.ie/en/smartmeters/)

2. CRU Smart Metering Programme (2019 – 2025)

The CRU programme is largely complete. Phase 1 delivered almost 1 million Single-phase whole current meters and associated infrastructure (HES, MDMS). Phase 2 has completed installation of over 1 million Single-phase whole current meters and associated infrastructure (HES and interface to existing MDMS) with more capabilities. Three-phase Whole Current metering installations, interfacing with the Phase 2 HES has just begun.

2.1 Phase 1 Summary

Phase 1 included the installation of nearly 1 million SEMs, along with two Retail Market Schema Releases. At present, all systems, business and retail market changes are completed to allow 30-minute interval data to flow to Suppliers via the Market Systems and for Interval Data and a new 3-part TOU Standard Smart Tariff to be used in all market processes including DUoS Billing and Market Settlement Aggregation.

The Smart Meter and the associated backend IT Systems were procured to facilitate the Smart Meter rollout for Phase 1. This rollout began in Sept 2019. The Smart Metering solution which has been deployed consists of the Kamstrup OMNIA Power Single-phase SEM, the Kamstrup OMNIA Head-End System and a private APN on the 3Ireland network.

A Meter Data Management System (MDMS) has also been procured and deployed during Phase 1. This is the Siemens EnergyIP MDMS. The Kamstrup HES and the Siemens MDMS are integrated using the Common Information Model (CIM) v2.0 (International Electrotechnical Commission (IEC) 61968-9) interface.

2.2 Phase 2 Summary

Phase 2 delivered the installation of an additional 1 million SEMs. In addition, a Smart Pre-Payment solution has been delivered in this phase. This solution is based on a Thin Pre-Payment model where all balance calculations and customer balance / top-up communications are performed in the Supplier backend IT systems. The Smart Meter will have no specific pre-payment functionality – the same configuration will be deployed on the SEM irrespective of whether the customer has opted for a pre-payment tariff from their Supplier or not.

Note that the Smart Meters deployed in Phase 2 and Phase 3 of the project will support the full set of functionalities being enabled in Phases 2 and 3. Hence In-Home Data Channel is supported (and tested) in the Smart Meters deployed in Phases 2 and 3, and this capability is now being integrated into the wide range of ESB systems.

Phase 2 smart meters are supported by the Siconia HES delivered by Sagemcom, and this integrates into the Siemens EnergyIP instance delivered in phase 1.

2.3 Phase 3 Summary

As of March 2026, Phase 3 is currently in progress. This phase includes the installation of the remaining whole-current SEMs by the end of 2026.

Several key capabilities identified in the NSMP High-Level Design (HLD) are required to be enabled by the conclusion of this phase. These include:

- **In-Home Data Channel:** Provision of an in-home data interface from the primary SEM in the premises. This channel is intended to provide near real-time energy usage information to customer-owned devices (such as in-Home Displays). The current NSMP HLD assumes that electricity consumption data will be delivered through this channel.
- **Last Gasp:** The meter's ability to send an immediate outage notification when it loses power.
- **Meter Ping:** The ability to remotely query the meter to confirm its status and connectivity.

It should be noted that ESB was originally required to manage communications for smart gas meters. However, the CRU withdrew this requirement during 2024.

3. ESB Networks Implementation Overview

3.1 Introduction

This is new procurement process, therefore, represents a business-as-usual activity.

Across the EU and globally, metering technology, network infrastructure, in-home devices, cybersecurity requirements and communication platforms are evolving at pace. ESB Networks recognises that defining the specification for the next generation of advanced smart meters must be informed by this wider technological and regulatory evolution. Accordingly, before progressing to a future procurement for advanced next-generation meters, ESB Networks intends to undertake this procurement to address current operational needs and ensure the continued stability, performance, and security of the existing smart metering environment.

This procurement, therefore, will deliver:

- Single-phase whole current, Three-phase whole current and Single and Three-phase Current Transformer meters.
- A Head-End System (HES) capable of meeting ESB Networks' functional, security, and performance requirement for 1.5 million SEMs initially and the capacity to scale up to potentially 3 million SEMs during the contract, including:
 - Software
 - Installation services
 - Configuration and integration services
 - Security hardware and software to support the AMI infrastructure
 - Support and Configuration services

For clarity, ESB anticipates two or more Vendor(s) but may award to a single vendor:

- AMI systems vendor, responsible for the HES, HSM (if necessary), the MDMS adaptor, interfaces to other ESB and comms provider systems, and collaboration with meter Vendor(s) to integrate meters to the HES, throughout the entire life cycle of the HES.
- Meter vendor(s) who will integrate their meter type(s) into a HES, manufacture, preconfigure, deliver, and support the meters through the meter life cycle.
- Integration of meters from other manufacturers will be a key requirement of the solution even if a single vendor is selected.

3.2 ESB Project Model

The ESB PMO Framework is the end-to-end process for Projects to be delivered using a standard waterfall delivery methodology. ESB will manage the E2E programme and prospective Vendor(s) will be expected to provide project managers to integrate into the overall PMO.

The PMO Framework is based on the standard PRINCE2® method, but has been tailored to suit ESB requirements. There are six phases of the PMO Framework, each of which has mandatory deliverables and exit criteria which must be completed before the project can progress to the next phase.



Figure 1 ESB V Model

3.2.1 Concept Phase

The Concept Phase is the entry point of a project idea into the PMO Framework and is managed by ESB. The Key Objectives of the Concept Phase are: To evaluate and explore the Project Idea proposed by the Business, and to decide on Product or Project route via the 3 Delivery Options (1. Waterfall, 2. Agile or 3. Analytics). The outputs for Concept include Completed Project on a Page (POP), Costs Approved for Definition Phase, Project Scheduled for Definition and Resources Secured for Definition.

3.2.2 Definition phase

The Definition Phase evaluates and explores the project idea generated during the concept phase at a high level. Key Objectives of the Definition Phase are: To understand Why, What, How and When the project can be delivered; To clarify Business Requirements and agree the High-Level project scope; To prepare a High-Level estimate of resources, costs and timelines; and to prepare an Initial Business Case and ensure there is a clear justification for the project. The outputs for Definition include: Approved Project Brief Presentation; Approved Costs for Preparation Phase; Initial Business Case, and Resources secured for Preparation.

3.2.3 Preparation Phase

The Preparation Phase further refines and builds on the work completed during the Definition Phase. The key Objectives of the Preparation Phase are: To Agree the Project Scope; Prepare a Detailed Project Plan and Estimate for the Execution Phase; and Prepare and Sign off the Business Case and Project Initiation Document (PID). With the outputs for Preparation to include Approved PID, Final Business Case (incl. Budget and Benefits Realisation Plan), Detailed Project Plan for Execution, and Resources secured for Execution.

3.2.4 Execution Phase

The Execution Phase delivers the project in accordance with the plan developed during the Preparation Phase. The key Objectives of the Execution Phase are: Ensure that project control is maintained during the Design, Build, Test and Deploy stages; Manage and Control Scope, Budget, Risks, Issues and Quality; Agree Plan for Transition Phase. The outputs for the Execution include Successful Go-Live, and Plan for Transition Phase.

3.2.5 Transition Phase

The Transition Phase includes both IT Transition and Adoption and Change Management. Both elements occur throughout the Project Lifecycle and enable the transition to the Business and Support areas. The Key Objectives of the Transition Phase are: Agree and Develop the IT Transition Plan and Support Model; Understand the key Transition (IT and Change) activities that take place across the Project Phases and Sign off IT Transition Plan and Support Model prior to Project Go-Live. The outputs for Transition include Acceptance into Support, and the End of Project Report.

3.2.6 Knowledge Phase

The Knowledge Phase and its related activities occur throughout the Project Lifecycle and is central to continuous improvement and learning. With the key Objectives of the Knowledge Phase are: To capture Lessons Learned on current Projects and apply these to future Projects; and to enhance the PMO service going forward. The outputs for Knowledge include Lessons Learned Reports, and Updated Project processes and templates.

The Vendor(s) will be involved from the Preparation to Knowledge Phases of the ESB Stages. The following section provides the Vendor(s) with a high-level understanding of the scope of these stages and activities. The RACI and details for each of these phases will be shared as part of the ITT.

3.2.7 High Level Plan

The Figure below is a high-level Plan outlining the key stages and milestones of the Meter+ implementation. The following sections give a lower-level view of the AMI stages that relate to the scope of this PQQ and ITT process.

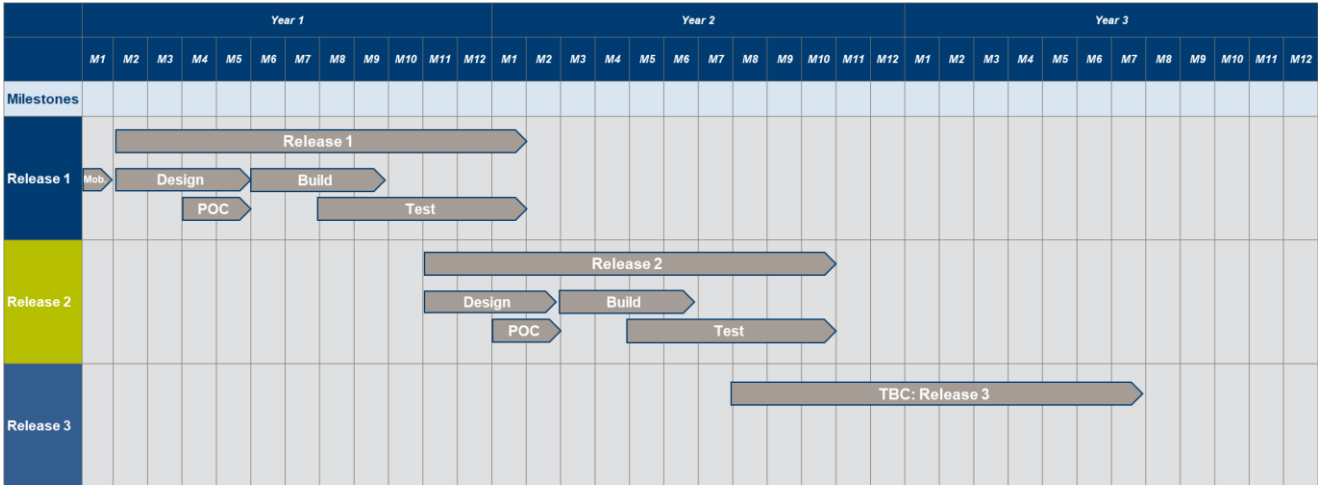


Figure 2 Meter+ High Level release plan

3.3 Scope of Meter+ Functionality Releases

The procurement delivery approach is expected to include a series of functionality releases to support the provision of SEMs and the Multi-Vendor Head-End System (HES) to the market and to deployment rollout teams. For planning purposes, it is currently envisaged that this may comprise of two primary releases (referred to as Release 1 and Release 2) and a possible third release. However, these releases are notional and may be refined, expanded, consolidated, or otherwise re-sequenced during the procurement process or subsequent delivery phases.

- **Release 1** – The scope of Release 1 is to enable the single-phase Meter+ meters and AMI backend systems to support existing functionality (i.e. Meter Configuration Code(MCC)s: MCC01, MCC02, MCC12 and MCC16, automated sending of meter logs, on demand reading, supply control switch operations, smart prepayment, Microgen export, in home channel enablement and disablement, and alerts for power failure (“last gasp”) and includes the integration to the MDMS.
- **Release 2** – The scope of Release 2 is the addition of Three-phase metering including extensive configuration of the advanced features of Three-phase WC and CT meters (for example, pulse outputs).
- **Possible Release 3 and subsequent releases** – Additional meter types, as well as other communication technologies, may be integrated, tested, and brought into service over the lifetime of the HES. Each integration activity will typically constitute a release.

3.3.1 Meter+ Release 1 Scope

Release 1 delivers a fully functional solution for the single-phase meters that are the priority for this implementation. The single-phase meters will be internally identical but will be delivered with two identities with differing initial configuration. Release 1 will include the following but limited to:

- Design, build and test of the MDMS adaptor, HES and new Meters.
- Meters using Narrowband Internet of Things (NB-IoT) and Long-term Evolution for Machines (LTE-M) communications.

- Device Language Message Specification (DLMS) Use Cases from ACE GCP with some modification.
- “Zero touch” installation data ingestion¹.

3.3.2 Meter+ Release 2 Scope

Release 2 is the extension of release 1 to support three-phase whole current and single and three-phase CT meters. The focus of this release would be the update required to the HES, MDMS Adaptor and MDMS to support the three-phase meters that will be installed at the end of the Design, Build and Test of Meter+ Release 1.

3.3.3 Meter+ Release 3 (and further releases) Scope

The HES is intended to be able to manage multiple meter types and purposes. Further releases may be required by ESB to initiate the adoption of other meter types into the HES, addition of different measurement and billing values to facilitate innovative tariffs and possibly allow the SEMs to provide enhanced functionality.

¹ Meter installers do not carry a HHT, and as such security credentials, meter identities have to be delivered from the meter vendor and be ready for use when the meter initiates its first communications.

3.4 Execution Phase

ESB wishes to draw all Vendor(s)' attention to the following information and summary of scope of these sub parts to the execution phase.

3.4.1 Meter+ Design Overview

ESB Networks envisage that the design work that would need to be undertaken would concentrate on the configuration of the proposed solution and the infrastructure design of the environments, not on the development of the HES SW. Part of the scope of this work is to fully document the product and the implementation of the product within ESB environments, to enable the operation, use and support of the product(s) by both ESB IT Services(ESB ITS) and ESB Networks. A key element in this design process will be the analysis of the cybersecurity of the solution to maintain ESB Networks IT/OT security. This phase will also include communication establishment and use case validation with the meter(s). As part of this design work ESB expect there to be workshops, training and system/product information created. These types of activities should enable ESB Networks and ESB ITS to understand the Architecture (Solution, Business, Data, Infrastructure, Technology, Service and Security) with the AMI HES Vendor and meter vendor(s) working with ESB Networks and ESB ITS to document these deliverables and ensure that they are in line with the requirements of ESB's final solution for both planned releases. This will require that all Vendor(s) are present on site for these workshops, meetings, documentation creation, design reviews, design complete and Go/No Go meetings. The operating model that ESB envisage is not a managed service. ESB expect to be able to support the AMI solution in house.

3.4.2 Meter+ Build Overview

ESB Networks IT systems are based primarily on Microsoft and Linux platforms and therefore the following considerations should be taken into account by the proposed solution provider for the design and build of the IT System requirements.

3.4.2.1 Consideration 1

It is expected that several Environments will be available to support the Design and Delivery of Meter+ releases. Development, Test, Preproduction, Production and a Training environment are currently employed. The Development, Test and Training environments will be scaled down versions of these but generally will provide the same functionality. AMI Smart metering will use ESB's established path to production outlined below. All deployments will be released to the development environment and promoted up through the environments once they pass the required test phase.

ESB requires solutions that demonstrate zero tolerance for service downtime. Proposed systems must employ highly available and resilient architectural approaches like containerised deployments and Microservices Architecture to ensure continuous operation. Solutions should support seamless, on-the-fly horizontal scaling in/scaling out and replacement or updating of services without interruption to business operations.

ESB requires that solutions should have proven Disaster recovery capabilities in-line with ESB's Business Continuity and Disaster Recovery (BCDR) requirements. For example, the Production Environment is replicated at a second Data Centre (Failover instance) and ESB regularly switch production operations from one data centre site to the other, swapping the Production and Failover

instances. The Production instance runs at the new site for a period of months following each site switch.

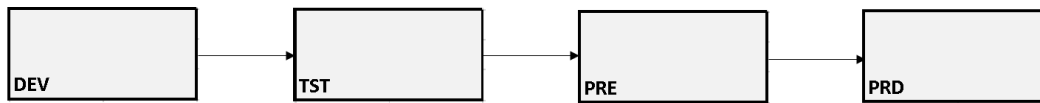


Figure 3 - Environment Promotion Path

3.4.2.2 Consideration 2

ESB assume that in order to increase the security of the solution the various components of the AMI solution will be hosted on different subnets or VLANs to further isolate the network. For example, the HES components will be segregated from the Key Management Services or the HES components managing direct communications with the SEMs may be segregated from the HES components processing the received data. The different components will communicate with each other by configuring only the necessary firewall rules needed to support the required traffic. Each component of the solution will have a separate instance for each environment hosted on the same VLAN. E.g. the non-Production HES VLAN will be shared by all non-production HES environments (Dev, Test, Preprod).

3.4.2.3 Consideration 3

Access to ESB AMI systems will only be available to onsite personnel during the Design and Build Phases. Remote access to the AMI infrastructure will not be permitted. All software and applications making up the AMI solution will operate on servers in the ESB dual Data Centres in Ireland. Any software delivery shall be via the approved by ESB secure mechanisms (e.g. SFTP). All software installs and updates will be completed by ESB personnel with assistance from the on-site software vendor personnel.

3.4.2.4 Consideration 4

Onsite times and days shall be in line with ESB's normal operating hours, and in line with Irish holidays, for all personnel assigned to the project.

3.4.2.5 Consideration 5

ESB Enterprise Architecture have developed a set of simple and easily understood principles that apply to all aspects of running IT in ESB. These are: Keep IT Simple, Manage Our Data, Enable Innovation and Agility, use what we have already paid for, Don't re-invent the wheel, Keep IT in support, Keep the Business running, Play by the rules.

ESB ITS supply the IT infrastructure for the Smart metering infrastructure to ESB. Therefore, the HES Vendor will work with ESB and consult with ESB ITS to agree the design of the Infrastructure within the design period and enable and assist onsite ESB ITS staff to install and Product Integration Test within the build period, whilst also assisting in the production of documentation (e.g. configuration setting, interface documentation, updates to the Architecture etc.) that will be required to exit the build period.

3.4.2.6 Consideration 6

In recent years, the energy sector has undergone significant transformations driven by technological advancements, regulatory changes, and evolving consumer expectations. As a leading utility provider, ESB Networks is committed to staying at the forefront of these changes to ensure the delivery of reliable, secure, efficient, and sustainable energy solutions. One of the pivotal components in this transformation is the update of AMI components and capabilities over time. Changes in rules (i.e. Measuring Instruments Directive(MID), EU Cybersecurity Resilience Act (Regulation 2847/2024/EU, supporting Directive 2020/1828/EU), Radio Equipment Directive(RED) cyber, EU Network and Information Systems Directive (Second version) (NIS2) and risk (e.g. from quantum computing, more data requirements) will apply and need to be addressed as part of vendor responses and capabilities.

3.4.3 Meter+ Testing Overview

As part of the Meter+ delivery model there is an expectation that the successful Vendor(s)' proposed solution is "off the shelf" and therefore, there is an extensive testing period that ESB will need to undertake to validate the features and functions of the AMI and meter elements to ensure that they are in line with contractual commitments and satisfy the ESB requirements. To this end an allowance must be made that a sufficient quantity of test SEMs and support will be provided to allow ESB the time and expertise for this validation to take place within each of the required environments. ESB will also require SEMs to be sent off site for independent testing (for example security penetration testing).

ESB has a defined test model that is detailed below. Each of the releases shall be subject to this process and to documented test gates, and only on completion of the successful exit of these gates shall the solution progress. In addition to the test phases called out in the V-model, ESB will be witness testing (a subset of the overall test cases to be tested) the execution that is undertaken by the HES for the AMI solution. Quality gates will also be in place to ensure the expected level of quality is achieved. Witness testing will be executed by the HES Vendor and witnessed by ESB within the HES Vendor PIT environment for AMI prior to the handover of code to ESB.

The following Table details the Testing types that shall be considered for each planned release:

Table 1 - ESB and HES Vendor Test stages

Test Phase	Description
Requirements Test	Validate that the Business Requirements and Test Conditions detailed in design documents meet standard criteria and form a basis for testing based on IEEE 820 standards
Unit Test	Verify that developed software units work as specified in technical specifications.
System and Interface Test	Verify that the developed solution as a system, including all interfaces between units, works as specified. Focus on new/changed functionality
End to End Test	Execute full end to end testing scenarios to ensure that the system is working as designed.
Performance Test	Verify that the system meets performance criteria
Non-Functional Test	Verify that the testing of an application for its non-functional requirements e.g. Security behaves as expected
Regression Test	Verify that an applied fix, modification or extension did not introduce new defects in other areas of functionality (usually related areas).
User Acceptance Test (UAT)	Verify that the developed solution works as specified in the business requirements and supports business processes as specified in the BPD. Focus on functional test of end-to-end business processes.
Back-up and Recovery Testing	As part of the resilience capability for ESB Vendor(s) will be required to support the testing of various recovery processes and technologies.

Security testing is applied across all test phases. ESB recognises that confidential data is available across environments. Access is restricted in all environments, and a secure configuration is applied. Test environments are reflective of production.

3.5 Transition Phase

ESB wishes to draw the Vendor(s) attention to the following information for the Meter+ Transition Phase:

3.5.1 Operation Life

There are two key elements to the operational life support that are required from the solution offering.

3.5.1.1 Hypercare

This is a period post the Go Live on the Release date. This will be a fixed period, to be agreed, during which the Vendor(s) are expected, on reporting of an incident, to confirm receipt of the incident and to then attend site within agreed timeframes to enable effective incident management.

Typically, it is expected that the Vendor(s) will have suitable support staff located in-country, co-located with ESB operations or project teams during this period.

3.5.1.2 Operation Support Services

This is the aftercare service offering for the product(s) that have been offered by the Vendor(s), and as such the level of the service will be agreed as part of the ITT. It is anticipated that the ITT will require options on the service level agreement and ESB may choose to have different SLA's dependant on the component (i.e. SEM vs. HES).

There are a minimum number of items that ESB would expect to see within the SLA and these have been grouped at this stage for guidance to the HES Vendor. Should the vendor have additional offerings, then these should be detailed within the ITT response.

- **Operational Services:** All communication services supplied by the HES will be subject to Service Level Agreements (SLAs). These SLAs will cover all the messaging across the HES system and the quality of what is being delivered against the operational business requirements. These requirements cover service performance, timing and availability as well as accuracy of data. Depending on the messaging type and version, these requirements will vary and the system design and software must be designed to achieve these SLAs. Performance against these SLAs will be constantly measured and adjustments made to optimise system operation to achieve these. They will then be formally reported monthly for supplier performance evaluation against the contract. In the event of non-compliance issues, then it is expected that the vendor will work with ESB to resolve these.
- **Product Application updates and patches:** It is expected that throughout the life of the system there would be a need to undertake Software/Application updates of the IT systems and meters as the applications evolve in line with the market. As such it is anticipated that the Vendor(s)' products would also need to be updated to fix discovered security problems or in line with other Vendor(s) (or third party) product roadmaps (e.g. Microsoft, Siemens, SAP, Java). Therefore, an understanding of the base applications that the AMI Product(s) utilise and the base applications' likely roadmaps for patches and releases is required, so that this can be planned for or mitigated. Each of the planned releases should be accompanied by full documentation to enable ESB to understand the release objectives and any inherent risks contained therein.
- **Feature Enhancements:** ESB is aware that the products that they will purchase through this process will be a standard offering that is under the control of the Vendor(s), which in line with their internal Roadmap, may add new features and functions. ESB requires an understanding and visibility of the internal roadmap throughout the operational life of the AMI System, as a function of the aftercare offering. This should enable ESB to either accept these new features or functions or continue with the current product offering. It is not expected that at any point the product would or could be marked as end of life, or that it would no longer be supported.
- **Vendor / Client Management:** It is expected that throughout the operational life of the system the Vendor will undertake review workshops and meetings. These workshops and meetings will keep ESB informed of any product developments and any new product offerings

from the Vendor(s), along with the normal Client vendor management operation, (e.g. Support call reviews, warranty claims, Account reviews, etc...).

- **Training:** As new features or changes to the products are offered it is expected that these updates or feature releases will be accompanied with the relevant training and documentation. It is also anticipated that throughout the life of the solution and project there will be a need to draw down on training and training material offered by the Vendor(s).
- **3rd party management:** ESB apply a strict vendor management process. This is aligned with the agreed vendor contract. ESB will monitor vendor performance in line with the contract, including the right to audit Vendor(s).
- **Resilience:** Resilience is a key focus area for all Regulators in the utilities industry. ESB will expect the successful vendor to support ESB in meeting its resilience objectives for Smart Metering. This support will cover but not be limited to operational resilience (including recovery from incidents) and cyber security in support of the NIS2 objectives that ESB is required to meet.

4. High Level Advanced Metering Infrastructure (AMI) Capabilities and Scope Features

4.1 High Level Capabilities

There are several business capabilities from the ESB Capability Model (a high-level framework representing everything an organisation must be able to do to achieve its goals) that are relevant to the Meter+ implementation and, by extension, to the Meter+ procurements. These capabilities inform the scope of the solution and help outline the high-level functions and system features required. For the PQQ, the information presented remains at a scoping and informative level only; full business processes and detailed requirements will be provided to the shortlisted bidders as part of the ITT.

The capabilities identified as being within scope for this PQQ and ITT are summarised in the bullet points below. The detailed definitions of these capabilities are provided in the Appendix for reference.

Table 2 – High Level Capabilities - Core

ID	Capability Title	ID	Capability Title
5.4.1	AMI Operations Strategy & Planning	5.7.5	Meter Asset Performance Management
5.4.2	AMI Data & Message Management	5.7.6	Meter Firmware Management
5.4.3	Manage Meter Data Retrieval	5.7.7	Device Configuration Management
5.4.5	Communications Service Management	5.7.8	Device Event & Alert Management
5.4.6	AMI Service Management	5.7.4	Meter Asset Testing
5.7.1	Meter Asset Strategy & Specification	5.7.5	Meter Asset Performance Management
5.7.2	Meter Asset Registration	5.7.6	Meter Firmware Management
5.7.3	Meter Asset Replacement Management	5.7.7	Device Configuration Management
5.7.4	Meter Asset Testing	5.7.8	Device Event & Alert Management

While all core capabilities of the Smart Metering capability model must be supported where relevant, the following supporting capabilities are anticipated to be of greater significance as part of a multi-vendor HES design. As with core capabilities, descriptions can be found in the appendix of this document and documentation will be available as part of ITT.

Table 3 – High Level Capabilities – Supporting (Selected)

ID	Capability Title	ID	Capability Title
1.9.1	Security Oversight and Cyber Risk Management	1.9.3	Identity and Access Management
1.9.2	Data Privacy and Protection	1.9.4	Security Operations, Vulnerability Management and Incident Response

4.2 High Level Scope Features

While the above capabilities are required for the support of the ESB Networks Meter+ procurement. This PQQ calls out several key features that ESB wish to offer for tender, therefore, the following points should be considered as the high-level scope for the features of the complete AMI Solution:

4.2.1 General

The interchange between the SEM and the HES will be based largely on the DLMS User Association AC Electricity Generic Companion Profile version (hereinafter referred to as the ACE SM GCP), with optimisations for security and other features needed to meet ESB Network's and the Irish Electricity Market's requirements. ACE SM GCP is a DLMS/COSEM-based companion specification defining the standardised data model and interoperability framework for SEMs.

4.2.2 Tariffs

There are a number of tariffs (N.B. These do not contain costs per KWh but are only the register configuration and timings) that are currently supported within the Market; these consist of a number of variants that are either based on Non-interval (A+,A-,R+,R+ and ToU rates 1-4) reading or interval readings (average Import and Export Power and either 48 x 30min or 96 x15min intervals) to create a reading set for the day.

These tariffs need to be switchable via a remote command Device Market Configuration (DMC) from the market in accordance with UC02 of the ACE SM GCP. The SEM and HES should record information that is relevant to this process to confirm that this update, or activation of any new Tariff, has been triggered or undertaken.

While the creation of the tariff is one part of this use case, the other is that of the information that is required by the system every night for the purpose of billing data. As such upon the change of a Tariff the information that the SEM sends as part of the Billing data should also be reconfigured to support the relevant registers. This is delivered using ACE SM GCP UC05. Ensuring that the data that is transmitted from the SEM does not create a GDPR breach.

Therefore, the configuration of the billing information, and the method by which it is transmitted (e.g. push or pull), shall be configurable and controlled through a set of Meter Data Protocol messages sent from the HES, in line with the tariff that has been applied to the SEM.

All relevant SEM events (e.g. power, time, etc) that are required to be able to validate these reads should also be available for transmission on to the Siemens MDMS to enable the Validation, Estimation and Editing (VEE) processes.

4.2.3 Estate / Device Management

As part of the AMI Solution the HES shall be able to control and manage the SEM(s) SDC (Smart Device Configuration) and report on the current and historical changes that have been applied to the SEM over the operational life of the meter. This configuration should include all remote settable parameters, current and pending, hardcoded parameters and communication information relevant to the operations of the estate management.

The HES shall also include the ability to manage and control the applied configuration (including tariff), firmware and hardware standard on every SEM deployed. The HES will be capable of ensuring that the communications only go to authenticated SEMs that can operate correctly and that any changes of firmware and/or configuration are carried out in a secure process that can be configured by ESB operators. This will include the sequencing of upgrades and dependant on others and ensuring that only relevant updates are carried out on SEMs that have the correct product, hardware, firmware and configuration.

The AMI System and the HES shall be able to manage and maintain the ID's required within the system to allow for communications between the back-office system (i.e. MDMS and SAP) and the devices within the consumers home, along with the necessary Meter Data Protocol (MDP) message required for change to these IDs and management of these devices. As the DLMS UA ACE SM GCP 1.0.1 has been adopted, then the security will use DLMS Suite 1 and 2. The proposed MDP should ensure that all communications are secure and authenticated both by the source and destination of the MDP. It is ESB's preferred option to have an MDP based on certificates as this method of authentication and authorisation, however all other equivalent security solutions will be considered.

The HES and AMI Solution shall be able to maintain accurate time within the AMI System, from HES to Meter. This is necessary to ensure that each meter maintains accurate time and correctly records energy consumption/export into the appropriate intervals and accurately timestamps register snapshots and meter events. To facilitate this, the ACE SM GCP UC07(DLMS Use Case 07) will be used, the HES is expected to support both the direct clock adjust scenario and the Network Time Protocol (NTP) scenario.

4.2.4 Local Data connections

There are several connections that the SEM must support for the transmission of data either to the home or to the operational Systems. Figure 4 below shows these connections.

The WAN connection is the main route for data exchanges between the SEM and HES. While this is the main route there is also that of the manual read and the Handheld Terminal (HHT) read that should be a feature of the system. The HHT should allow the system to take readings and data exchanged between the HES and the SEMs and ensure that the transmitted or captured information is shared with relevant parties within the AMI System. Note, where an app is required, iOS is preferred.

Note. HHT will act as an alternative WAN and therefore use secured messages from the HES to move to the SEM and vice versa, rather than generally generating commands itself. It is expected, therefore, that HHT functionality will require some development to comply with the ESB security architecture. The Local Data connection is an Optical Port compliant with IEC 62056-21.

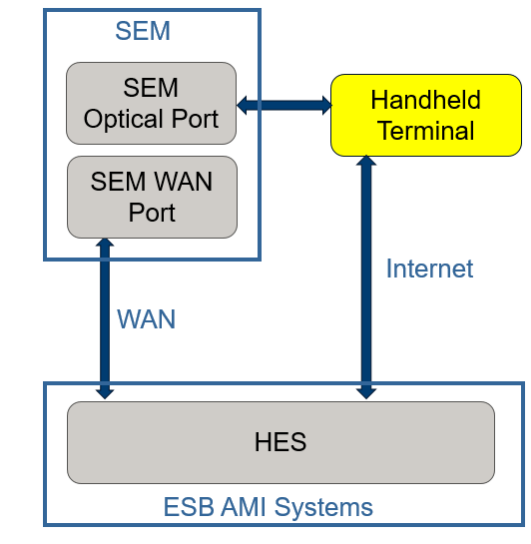


Figure 4 High Level SEM Component Interfaces

As part of the HES and SEM there is a requirement to undertake several operations local to the SEM. These cover general maintenance and operations where a SEM is not in the WAN coverage and requires configuration, firmware update, readings, or investigation, and as such the local data connection should enable ESB Networks to create a secure local connection to the SEM to undertake these activities. The Solution should offer a secure method that allows for authenticated and authorised MDP messages to be exchanged, whilst not compromising the security of the solution or the SEM. This, therefore, is not a straightforward implementation of ACE SM GCP UC19.

In addition to the local connection, the solution should also enable the consumer to access metering data that has been defined within the SEM via the companion specification as a subset of the overall SEM capability to allow the consumer to understand their consumption data usage. This local connection should be configurable through a set of parameters that allow for change should there be change in consumer (Change of Legal Entity (CoLE)) served by the SEM or change in the national regulations. This customer data will be provided using a wired port applying the DSMR P1 Port specification.

The local connection should have security methods available to the HES to manage the change in supplier or consumer. There shall also be a method by which ESB is able to understand the connectivity parameters and characteristics of the devices connected. This is managed using ACE SM GCP UC12.

4.2.5 Instrumentation and Smart Network Management

ESB Networks endeavours to provide supply conditions in accordance with the EN 50160:2010 EN 50160:2022 + A1 :2025. To accomplish this, the SEM and HES will be required to monitor Voltage, Frequency, and Harmonic parameters for low voltage. In addition, to provide further understanding of the network conditions, the SEM and HES will be required to monitor other parameters that can have an influence on Power Quality, and these are active power, reactive power, demand, current and phase angle and other SEM condition parameters as required. Several functionalities are anticipated in the SEM and HES with respect to monitoring parameters, and these are time and value thresholds for recording excursions from normal conditions, recording of the time and duration of excursions, maxima and minima for the parameter, and logging of the average and other values of the parameters. Further details of the SEM performance requirements will be included in the SEM specification. The HES shall be capable of enabling, disabling and configuring any of the thresholds, logs and event actions (including alarms/alerts) that may be required by the SEM specification, and configuring the SEM to push data and manually collect the data as required by applying ACE SM GCP UC08, noting that some additional measurands are required.

A series of Thresholds is required within the SEM to generate different types of Events. Whenever the Event Logs indicate locations where these Events are common, then a 10-minute voltage profile covering the previous 3 months, which is being recorded in the background on the meter, shall be able to be collected on demand or via a campaign to help with the analysis of the quality of the power supply in that location.

The SEM shall have two High-Voltage and two Low-Voltage Thresholds (i.e. configuration items settable by a DTC command). When these thresholds are crossed then the SEM shall record an Event. The SEM shall be capable of sending an Alert to the HES when an Event is generated. Events and Alerts shall be processed by the HES and forward to the other ESB AMI components and MDMS for further processing, the HES should be able to generate a report on these events and alerts for review per period (i.e. daily, weekly, monthly). This information should also be available via a HES UI.

In addition to these Thresholds, there is also a requirement for the SEM to have a configurable Voltage and or Current Profile at an interval of 10 or 30mins for up to 3 months. The HES should be able to create ad hoc reads of this profile data across the entire estate if necessary, and be able to process this request, in addition to the normal operations of the System. This should be viewable via the HES UI and for forwarding via the HES API.

In addition to the Thresholds and Profile data that the SEM can transmit, there is a need to be able to manage the Events and Alerts that relate to the Instrumentation and Smart Network Management of the ESB Network. It is expected that the solution can enable/disable, configure event parameters, enable/disable alerts in accordance with the ACE SM GCP UC08 and UC16 for the following events:

- Smart Outage Alert / Last Gasp capability
- Power Down / Power Up Events (including first breath)
- Short term Over-Voltage and Under-Voltage excursions
- Rapid voltage change – Sags and Swells

- Power Factor
- Total Harmonic Distortion (voltage and current)
- Frequency variations (not expected to be significant)

Each of these event/alerts should create a report and be accessible via the UI and API.

4.2.6 Firmware (FW) and Configuration Management.

Through the operational life of the AMI Solution there will be requirements for the evolution of the system, components and products.

The FW and Configuration management feature covers both that of the SEM including communications functions and, in the future, that of the other AMI Components that are required.

4.2.6.1 SEM Configuration Management

Configuration management, while key to the operational and estate management of the SEM, is a key feature of the Solution. However, this should be configured as a pairing between the HES and the SEMs. As such ESB requires the following set of configuration capabilities within the HES, which can be assigned within the SEM.

4.2.6.2 Tariff Configuration

This configuration group or sets of configuration items, should include the calendar by which energy flow is configured to support Time of Use tariffs. This should be able to support current and future configuration for up to four Time of Use rates across either import and/or export energy consumption. It is anticipated that the Tariff calendar would be able to operate in either UTC or local time and be able to deal with the Summer and winter time switch overs without external interaction. A minimum of eight Day profiles allowing for twenty-four switching points, two-week profiles and four-season profiles would be required to cater for the current configurable ToU Tariffs that are offered in Ireland, and therefore the current and future Calendars, should as a minimum support these configurable settings.

Consideration should be to allow up to twenty special days per year that are pre-programmable and have the capability to use wild cards to allow for repeatable values (i.e. Good Friday, or Summer and Winter Time Start/End etc).

The below table gives a current overview of the tariff types that are currently in operation within Ireland. While this is the current view, the proposed solution should be able to cope with additional tariffs through remote HES initiated commands to create new tariffs without the need to apply a new FW to the SEM or HES. It is anticipated that all these tariffs will be in operation in the initial period of the deployment and, therefore, the HES should be able to identify the SEMs that are currently operating these different tariff types and use this metadata as reporting and query parameters.

MCC	24 Hr	Day	Night	NSH	Wattless	MD Normal	MD Peak	Cum Nor	Cum Peak	QH IMP kW	QH IMP kVAR	QH Exp kW	QH Exp kVAR	Import HH kW	Import HH kVAR	Export HH kW	Export HH kVAR	Import 24hr kWh	Import 24hr kVARh	Export 24hr kWh	Export 24hr kVARh	MD 24H	CUM MD 24H	Day Off-Peak kWh	Night Off-Peak kWh	Peak kWh	24hr (EXP) kWh	24hr (EXP) Wattless
01	X																											
02		X	X																									
03	X			X																								
04		X	X		X																							
05																												
06		X	X		X	X	X	X	X																			
07	X			X	X																							
08	X				X																							
09																												
10										X	X																	
11										X	X	X	X															
12														X				X										
13														X	X			X	X									

A Billing Set is required from all SEM stated on the Data Collection Schedule to be delivered to energy suppliers each day. ESB perform validation on readings prior to issuing data to energy suppliers, in addition to performing estimation on missing data, i.e. ESB is obliged to provide Energy suppliers with a full Day's Data for all customers registered to that supplier whether estimated, recorded, or collected. Today being Day X, ESB will provide 100% data for all customers to energy suppliers on Day X+1 (tomorrow).

For ESB to discharge its obligations, ESB requires a full and valid "Billing Set" for all customers on the Data Collection Schedule for the previous day no later than 03:30 local time on Day X+1 such that ESB will be in a position to complete data processing for all customers.

As such, the Billing Set for each SEM "Day X" must be delivered by the SEM to HES by 03:00 the following day (Day X+1). It is imperative that a DCP is requested from each SEM on the Data Collection Schedule after 00:01 on Day X+1 as this ensures that this DCP contains the end of Day X midnight validation readings. The DCP containing the midnight validation reading in aggregate with all other DCPs collected from the SEMs throughout the Day X (where applicable) constitute a valid "Billing set".

Due to the daily volume of data to be transported by the AMI System, ESB will allow the HES to collect DCPs from SEMs at all times (24 hours) – however as previously stated, each Billing Set must include the midnight snapshot and for a Day's Data to be valid, all data relating to the calendar day must be delivered by 03:00 on Day X+1.

A SEM may be deployed in an area in which no communications coverage is available, the SEM will however continue to log usage. The SEM has the capability to record, register and store data logs for up to 130 days with each event log having the capacity for 1000 events. As such the DCP may vary in size.

To ensure that either the HES or the CSP Network is not flooded with transmission at 00:00:00.000 the proposed solution should manage the retrieval of these billing sets through the HES Data collection schedule (e.g. SEM Jitter for transmission or HES Schedule Collection Pull windows). These methods for control should be configurable via a set of configuration items either in the HES or SEM via a remote command.

4.2.6.4 Events and Alerts Configuration

As part of the SEM there are several events that should be supported to enable the effective management of the SEM Estate and device (e.g. Power On/Off, Reset, Error, Clock Set/Sync, etc²). Each of these events should be configurable to be captured within the relevant log. These events should, as a minimum, have the time, event id and additional metadata captured to assist in the understanding of why this event has been created. The events that are captured should also be able to be turned on and off at the event level, and not the log, through a HES command. Each of these events should also be capable of being configured as an Alert, i.e. an event that is pushed to the HES at the point in which it is created. Again, this configuration should be configurable using a HES

² please note that a full minimum set of events will be detailed as part of the ITT documentation pack.

command in accordance with the Use Cases in the ACE SM GCP. The SEM should, as a minimum, support events to assist in the following areas:

Estate and Network Management: Events that relate to the current status of the SEM (e.g. Power On /Off, SEM Reset etc) or to the communications Network Management of the SEM (e.g. PDP Attached/Released or HES Connection via WAN or Local Data Connection, etc.).

Configuration and FW Management: Events that relate to the download or Activation of FW; or that relate to the change in configuration of the SEM, should be recorded when they are performed remotely either via the WAN connection or the Local Data Connection. As part of any of these processes these events should be accessible within the HES so that other AMI System components are able to correlate these events and activities within SEM Performance Metrics, for additional trend analysis. These events should be transmitted back to the HES as part of the action.

Metrology Recording: Events that relate to the capture of Consumption information that will be used by the AMI System to validate the Billing Sets each night (e.g. Time Set, Clock Sync Major or Minor, Power Off/On, Reset, Error etc..). These events would be required to be transmitted back to the HES each night and would be used for the VEE processing of data within the Siemens MDMS.

Other Events: Additional Events should be available within the SEM for transmission or collection by the AMI System on demand.

The ACE SM GCP has several use cases, notably UC16, which govern events and alerts.

4.2.6.5 Head-End System (HES) Configuration Management

The HES shall be able to manage the configuration of the Device estate; this is known within ESB as the SDC or Smart Device Configuration. The HES shall be able to record and change the SDC of a device based on either a request via the MDMS Adaptor or through the UI and API.

MDMS Adaptor: The HES shall be able to process SDC part requests that control the DMC parameters via the MDMS Adaptor. The DMC of the device controls the Market or Tariff configuration of a device. Upon the request the HES should process these in line with the execution time stated within the request, i.e. now or in the future, it should also record all activities that are carried out in performing the DMC within the Device, (i.e. HES Events).

UI: The UI of the HES shall enable the authorised and approved user to manage, report and configure the SDC of Devices that are supported by the HES.

API: The API of the HES shall enable the HES to share information about the SDC and its sub parts with external AMI components, so that the configuration of devices can be used as a feed for Device Performance metrics and trend analysis.

4.2.6.6 FW and Configuration management

The HES shall be able to manage firmware and configuration, and report on the FW and Configuration information held within the Smart Metering Estate and the Head-End System. There shall be a UI or Set of Views that allow an approved and authorised user of the HES to understand and manage all aspects of FW and configuration Management. Which includes, but not limited to

anything from Approvals of new FW into the HES FW Store, reporting on the current or Historical FW and Configuration Estate / Device FW and Configuration Estate, through to the creation and management of FW and Configuration Campaign types (i.e. Download, Activation or reading).

FW and Configuration Campaigns: The HES shall be able to manage and control the download of FW and Configuration. Devices covered by one or more FW and Configuration DL Campaigns. While this DL is being undertaken by the HES and AMI System there should not be a degradation of the normal service by the HES, nor should there be a reduction in the activities that the HES is able to undertake. The HES shall be able to create FW and Configuration Campaigns that relate to the:

Download: A Campaign that relates to the transmission of a FW and Configuration Package to a quantity of SEMs or Devices. This contains approved FW and Configuration with security features to ensure that only approved FW and Configuration for that Device is applied.

Downloaded in the right sequence and observes all of the dependencies for application and activation, e.g. Security applied by the HES and FW Package to denote that it has come from an approved ESB AMI System and observes the dependencies listed in the firmware release notes and SEM supplier requirements

Activation: A Campaign that relates to the transmission of a FW activation command to a quantity of SEMs or Devices. This contains approved FW activation command with security features to ensure that only approved FW for that Device is activated, e.g. Security applied by the HES to the command to denote that it has come from an approved ESB AMI System, and it is only for the activation of this FW on this device.

Status: The Active Reporting of the current FW that is operating on a SEM or Device.

FW Reporting: There should be a default set of reports that cover the capabilities of the HES and the management of the FW.

FW UI: There should be a UI that enables a HES Authorised and Authenticated user to understand, manage and review all or part of the FW Management. As a minimum there should be a UI for the import of FW to the HES FW Store for the creation and management of a FW Campaign, and the creation or running of the FW reports.

FW Store: The HES shall be able to store approved Device FW within one of its components. This shall be stored with reference data that allows the system to understand the device type that it is applicable to, the version information, and all other relevant information that the system requires it to be able to use the FW as part of a FW Campaign.

4.2.6.7 Campaign Management

The HES shall be able to operate campaigns that are either created based on a number of data items that are contained within the HES's Data model, or from an external interface (i.e. API and CSV import). These campaigns shall be used for the transmission of data (e.g. configuration, FW and reading collections) to the Smart Metering Device Estate; this can be for one or more SEM's, or other Device Types. The Campaign Management is expected to have a reporting set, along with management and control UI's within the HES, that allow an authorised and approved user to undertake the planning and creation of Campaigns, whilst also giving a view of the current status of

the campaign and the device status of the Devices contained within the campaign. There should also be a capability to understand the historical campaigns that have been operated and the devices that these contained and the outcome. These historical campaigns should be viewed as metadata that can be used for the creation of new campaigns. It shall be possible for the HES and the design to operate multiple campaigns simultaneously, so that the Smart Metering Estate is able to operate different types of campaigns to cover the entire estate. The Campaigns should be configurable both for the creation (i.e. Qty of Device, Campaign Type, Max Time Period, retry etc..) but also within the events created and reported.

Campaign Reports: There shall be a report for the overall status, along with a detailed report allowing a user to understand the message exchanges between the HES and the Device(s).

Campaign Events: There shall be events that detail success and failure of the campaign, and the devices within the campaign. Should a device or campaign fail then there shall be relevant metadata to explain the cause for the failure and therefore allowing a user of the HES UI or Reports to undertake investigation on the systems or device(s).

Campaign Type: There are a number of types of Campaigns that ESB envisage that would be undertaken in the operational life of the system.

Firmware Download: This is the transmission of the Firmware to the Metering estate; this is normally pre-planned to be downloaded over a set period of time that could be future dated.

Firmware Activation: This is the transmission of a command to the individual device as an authorisation to now use the downloaded firmware, this command will always be future dated.

SDC: The SDC (Smart Device Configuration) is one of two types, DMC would normally be undertaken via a remote command individually to the device and therefore should be viewed as a real time request for a campaign. Whereas the DTC would normally be scheduled through the system as a campaign similar to that of Firmware activation.

Read Collections: The Reading collections campaign should allow the user to configure an ad-hoc read of any metadata of the Device Estate, so that the information can be scheduled and collected. (e.g. Nightly billing data or Instrumentation data for ESB network management)

Campaign Interfaces: The HES shall allow for the campaign to be created and reported on via two major interfaces; the HES UI and the HES API. These two interfaces shall enable the user or external system to understand in real time the status and outcome of any active or historical campaign that has been undertaken, in operation or scheduled to occur. These interfaces shall allow for the creation, pause or cancel of a campaign. Therefore, the HES shall be able to create events that relate to these actions and make these events available to be used within reports or interfaces. There should be a standard set of parameters used for the creation and control of these campaigns within the HES.

4.2.6.8 Software Releases

As the Head-End System is normally a set of software components created to delivery as set of features³. ESB expect that over the life of the system some of these software components will require updates and/or upgrades to the base OS or applications, or as a result of new features or functions of the Product (i.e. HES).

Therefore, all releases of the HES should be accompanied with a set of documentation that details the full scope of the Software release and the inter-dependencies on other software or operating systems (including a software bill of materials). It is expected that the HES Vendor will be able to validate that the release of the Software will not cause operational problems with the system, should ESB choose to adopt the release offered. ESB anticipate that there will not be more than one major release of the Product per year, while accepting that there may be a minor release per quarter.

All SW Releases shall undergo a formal acceptance and will be taken through change control and testing prior to release; it is expected that testing of a release would take between 1-3 months dependant on the scope of the update.

4.2.6.9 Feature Development

As part of the operational life of the AMI Systems and the HES there will be a need to create new features for the HES and the Devices, therefore, the control for the creation of configuration changes should be under the control of ESB, with advice from the HES Vendor. Should the Feature require new SW or FW for either the HES or the SEM then ESB shall be able to request development of this via the ESB Change control process.

4.2.7 Security Management

Smart Metering has transformed the interaction between consumers and the energy market providers. It generates volumes of rich data to enable consumers to make informed decisions about energy usage. These advantages introduce a certain amount of risk that ESB networks has to manage. Privacy standards are well defined for smart meters with guidelines available on the privacy risks associated with granular customer consumption data and the recommended approach to address these concerns.

Security solutions continue to evolve across the globe as different markets have different requirements which have led to a diverse approach in achieving AMI objectives and the associated security and privacy goals. AMI stakeholders continue to work on a universal standard for Smart Metering as described in the European M441 Mandate and its successors which has created a baseline for Vendor(s) and operators to work off. The Smart Meter Security Architecture describes the enduring process required to maintain the security model in the face of a continually evolving risk and threat landscape. With the introduction of Smart Pre-Paid functionality, the ESBN smart meters are included under the NIS2 regulation and Vendor(s) will be required to support ESBN in their cyber security submissions to the Ireland National Cyber Security Centre.

³ Features as described within this document, and in line with the Vendor(s) AMI Solution Offering.

4.2.7.1 Governing Regulations and Meter+ Principles

Some applicable lawful regulations include:

- Irish Data Protection Legislation (Including GDPR rules from 2018)
- NIS2 EU Directive 2022/2555
- Cyber Resilience Act 2024/2847
- RED Cybersecurity Delegated act 2022/30
- ESB Networks Meter+ smart metering requirements
- ESB Networks Meter+ smart metering high level design
- ISO/IEC 27001 – Information Security Management Systems – Requirements

The privacy and security aspects of these regulations apply to the Security Guiding Principles adopted by ESB Networks during the scoping and design of security for the end-to-end AMI solution. ESB expects to operate secure lifecycle management including but not limited to:

- Secure sourcing and supply chain
- Software Bill of Materials (SBOM)
- Disclosure of vulnerabilities and securities flaws and roadmap for resolution

The security principles below must be adhered to at all times and are aligned to the ESB Networks Smart Meter High Level Design and Security Requirements:

Confidentiality and Privacy

- Integrity
- Availability
- Authentication and Identification
- Authorization
- Non-Repudiation
- Auditing and Accounting
-

4.2.7.2 Confidentiality and Privacy Principle

Confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. It ensures that any desired resource is only accessible under the designated conditions.

The components (including but not limited to HES, HSM, KMS, HHT and SEM etc.) of the AMI Security solution which enforce this principle are concerned with ensuring that data is collected, stored and transmitted securely so that only those authorised to use the information has access to it. Cryptography is used to enforce this principle, using strong encryption of data while it is in transit, strong access controls on all components of the infrastructure (including on-going enforcement of minimal access rights required to carry out a given role), deletion of data which is no longer required and compliance with Data Protection Law etc.

4.2.7.3 Integrity Principle

Integrity ensures that any desired resource contains accurate information and performs precisely as intended. The components (including but not limited to HES, HSM, KMS, HHT and SEM etc.) of the AMI Security solution which enforce this principle shall look to ensure that data cannot be modified while in transit by any unauthorised entity. They shall also ensure that any modifications carried out by authorised entities are fully audited and can be proved to have been carried out by the recorded entity. Authenticated encryption is used to protect data in transit and strong access controls combined with comprehensive and regularly reviewed audit logs are used to protect against and detect unauthorised modification of data.

4.2.7.4 Availability Principle

Availability ensures that the desired resource is available at the time it is needed and that it is accessible in the intended manner by the appropriate entity. The components (including but not limited to HES, HSM, KMS, HHT and SEM etc.) of the AMI Security solution which enforce this principle are primarily concerned with disaster recovery and preventing (or at least detecting and mitigating) denial of service attacks against the AMI infrastructure. The proposed security solution must be capable of dealing with automated failover to standby/backup infrastructure in the event of a disaster without any loss of system functionality or any lowering of the security posture.

In addition, the proposed security solution must detect denial-of-service attacks or other events which could lead to degraded performance or total loss of availability and must take automated action to remove or bypass the source of the performance impediment. An Incident Response program for the end-to-end AMI is necessary. This is to ensure that ESB Networks is able to detect, respond and recover from a cyber-security or communications incident.

4.2.7.5 Authentication and Identification Principle

Authentication and Identification ensures that any entity accessing any component (e.g. HES, HSM, HHT and SEM) or data structure (e.g. HES Database or SEM Object Model) within the infrastructure can be uniquely and completely identified. This is one of the core principles of any security policy – without the ability to uniquely identify a given entity wishing to interact with the AMI, it is impossible to enforce many of the other security principles described here. The use of usernames with strong

passwords (i.e. HES UI), digital certificates and digital signatures are some of the mechanisms used to authenticate entities within the infrastructure. Multi-factor authentication is to be used.

4.2.7.6 Authorisation Principle

Authorisation ensures that an authenticated entity is given access only to those infrastructure elements, system components and data structures for which access have been specifically approved. Again, this is another of the core security principles. Authorisation works alongside Authentication to ensure that only properly identified entities gain the appropriate level of access to resources within the AMI. The authorisation principle ensures that all required resource access is formally approved and enforced across the entire infrastructure.

Authorisation is generally implemented through the use of granular security groups associated with specific roles, so that every resource challenge any entity attempting to access it for the appropriate authentication credentials (e.g. digital certificate, session key, password etc.). The authorisation features within the proposed security solution not only concern themselves with who has access to a resource but also with the level of access available (e.g. view / modify / create / delete etc.).

4.2.7.7 Non-Repudiation Principle

Non-Repudiation ensures that any action carried out on the infrastructure can only have been initiated by the entity identified by the auditing/accounting components and that the entity cannot deny having carried out the action. The non-repudiation principle will be critical in AMI environments where actions are carried out which impact customers or the operation of the electricity grid itself.

Instructions to disconnect/reconnect energy supply to one or more customers will be a feature of the Meter+ procurement. These actions if improperly executed could have significant consequences for customers and for the stability of the grid itself. Hence, it will be necessary to ensure that the proposed Security Solution only allows such actions to be carried out by fully authenticated and authorised users/systems. The mechanism by which these users/systems are authenticated and the mechanism by which the commands are processed by intelligent components within the infrastructure must ensure that the component executing the command can be sure that the command initiated from an authorised source. Digital Signing is an accepted method for providing such assurance.

4.2.7.8 Auditing and Accounting Principle

Auditing and Accounting ensures that system activities can be reconstructed, reviewed, and examined from transaction inception to output of final results. It also ensures that system controls are provably compliant with established policy and procedures. The Auditing and Accounting components (e.g. HES, HSM, HHT and SEM) of the AMI Security Solution must be tightly integrated with all the other components (e.g. ESB Operational Data Stores, AD etc.). Without auditing and accounting many of the other security controls are rendered less effective.

For example, it is not very helpful to know that some authorised user carried out a command which had a negative impact on customers without being able to identify specifically which authorised user carried out the command. Similarly, auditing and accounting of unsuccessful attempts to carry out actions can alert administrators to possible attempts to compromise the security of the infrastructure or to mis-configured processes.

4.2.7.9 Security Architecture offered by the proposed solution

The Solution offered should be able to apply these principles and should clearly document how these are met by the security features within the products offered. The solution should align to zero trust architecture and defence in depth principles.

Each of the products offered as part of the solution should be able to satisfy these high-level requirements:

- Provable device and user identity.
- Secure transmission of critical commands (e.g. supply control switch) in alignment with latest DLMS standards.
- Role based authorisation based on least privilege principle.
- Secure hardware architectures.
- Secure manufacturing and software development lifecycles.
- Secure device delivery logistics.
- Secure firmware upgrade and device re-configuration.
- Strong encryption of all data in transit (and where appropriate, at rest).
- Strong protections to ensure the integrity of data and to prevent replay of commands.
- Ability to refresh Certificates and or keys and update encryption algorithms.
- Intrusion detection and prevention.
- Comprehensive Security Event logging.
- Comprehensive security auditing coupled with regularly reviewed security policies.
- Processes to enable effective recovery from security incidents.
- End to End encryption from the SEM to the HES (i.e. implemented by the Meter Data Protocol with no intermediate translations or transformations)

The security services implemented by the Meter Data Protocol (MDP) should ensure that all communications are secure (encrypted) and authenticated by both the source and destination endpoints utilising the MDP. ESB prefers an MDP which implements certificate-based methods for authentication and authorisation; however other security solutions will be considered.

4.2.8 ESB Smart Metering Companion Specification

As part of the Smart Metering strategy there is a need to ensure supply chain security, and therefore, there is a need to have more than one meter vendor within this supply chain. This calls for a Smart Metering companion standard for communication between the Head-End System and the SEM both via the WAN connection(s) and also via the local data connection and other connections within the SEM to devices within the consumer's home.

To facilitate this need, ESB Networks have decided to adopt the DLMS User Association AC Electricity Meter Generic Companion Profile, with some additional attributes and some additional roles.

5. Smart Electricity Meters (SEM)

5.1 General

ESB will require Single-phase whole current SEMs, Three-phase whole current (WC) SEMs, Three-phase and Single-phase current transformer (CT) SEMs. The latter requirement will often be met using a Three-phase CT SEM with a single CT.

Basic meter specification:

- The meters will be used for import and export. The meters will in summary have the capabilities as shown below.
- Meter deployment is envisaged across the following customer segments:
 - Single-phase SEMs supporting domestic and small business use cases.
 - Three-phase whole current SEMs supporting higher demand residential and business use cases.
 - Three-phase CT SEMs supporting large LV load and specialist customer use cases.
- The Single-phase CT solution will be deployed mainly to agricultural locations.
- The SEM will be capable of communications with the HES either using an embedded radio or with an external Communications Function Physical Device (CFPD) installed to and sealed to the SEM.
- The SEM will be capable of provisioning relevant data into homes.

5.2 Basic meter construction and operation.

The four basic types of SEM are outlined in the table below. Note that it is an acceptable proposal that the Single-phase CT SEM requirement is met using the 3 phase CT SEM.

Table 4 – SEM Types

Type	Single-phase WC SEM	Three-phase WC SEM	Three-phase CT SEM	Single-phase CT SEM
Voltage	230 V	230/400 V	230/400 V	230 V
Max Current	100A	3x100A	3 x 5 or 3x 10 A	160A
MID class	B	B	C	B
IEC active recording	1	1	1	2

accuracy (62053-21)				
IEC reactive recording accuracy	2 (62053-23)	2 (62053-23)	1 (62053-24)	2 (62053-23)
Terminal arrangement	BS7856:2017	DIN	DIN	By arrangement
Auxiliary relays	1 or 2	2	2	By arrangement
Pulse outputs	0	0	4	By arrangement

Further details:

- SEMs will register active and reactive consumption in both import and export direction.
- The three-phase SEMs will be capable of recording $Q_{i..Qiv}$ values for kvar.
- The meters will be capable of recording Time of Use based tariff registers and will be capable of remote configuration of these tariffs. The SEM will be capable of recording maximum demand conditions and times of occurrence with Time of Use activation and be capable of resetting these conditions by remote command or on a schedule.
- The meters will be capable of recording average power import and export values to a precision and accuracy suitable for billing, such that when the average power values are integrated over a day, they will total the exactly the same as the corresponding increment in the related import or export register.
- The SEM will operate at the required accuracy class where the air temperature may be in the range of -25°C to $+40^{\circ}\text{C}$ and will be capable of operating normally over its required life in humidity up to 95%, noting that condensation may occur on the SEM.
- The SEM will be capable of being installed in indoor locations or in outdoor meter cabinets mounted or recessed into external walls. In particular, the SEM shall be certified to IP54 using the process described in IEC 62052-31.
- The SEM will be constructed, type tested, certified, and unit tested in accordance with appropriate European/IEC standards in the series 50470 and the series 62052...62055 and other appropriate international and European Standards.
- Meter terminals will be of a twin-screw type with hardened screws. The terminals will be constructed of durable metal that does not react with copper.
- The SEM will measure temperature within the meter, ideally at the supply and load terminals.

- All components associated with the metrological operation of the SEM shall be located under the main cover and protected by one or more mechanical seals. The base and covers of the SEM will be fire retardant and comply with the IE EN 60695-11-10 Standard to a V-0 level.
- The SEM will be equipped with an “optical” local interface in accordance with IEC 62056-21.
- Whole current SEMs will contain a Supply Control Switch at the output of the line circuit capable of 10,000 operations and rated to 100A per phase, in accordance with IE EN IEC 62052:31 Use Case 3, and auxiliary switch(es) rated for 230V, 2A and 15,000 operations that can be controlled by the enhanced meter functions to facilitate the control of Night Storage Heating (NSH) systems and other applications.
- The SEM will be constructed (and integrated with any required Communications Function Physical Device (CFPD)) in a factory that manufactures SEMs in accordance with MID requirements, and each SEM will be tested and certified for compliance with the MID and for correct function of non-metrological functions.
- The SEM (including and Communications device) shall consume less than the requirements of table 6 of IEC 62052-11:2020 and this electricity shall not be chargeable to the consumer.

5.3 Communications

The SEM will be capable of communications with the HES using LTE NB-IoT Cat-M IoT technologies compatible with Cellular Radio networks deployed or planned and regulated in Ireland, and the SEM will use DLMS/COSEM in accordance with IS EN IEC 62056 series of standards. The SEM Comms shall identify themselves onto the cellular network using a softSIM or eSIM to hold the International Mobile Subscriber Identity (IMSI) and related parameters, and the device shall be capable of roaming and/or having the eSIM/softSIM remotely re-provisioned for an alternative network.

Note: The vendor will be responsible for the licensing of:

- any 3GPP technologies
- any proprietary technologies

The SEM will be capable of controlling the radio access technology applied, this will include setting priority to the radio technologies, disablement of technologies, etc.

The SEM shall be capable of providing contemporaneous⁴ data autonomously to the occupier of the premises using the DSMR P1 Port physical interface that is configurable from the HES in order to:

- Enable or disable the data provision.
- Protect the attributes using encryption and authentication.

⁴ The port will not be capable of providing historical records (that is, interval data or event data)

- Select the attributes to be provided and the interval between the provision of attributes.

The communications may be delivered in one or more modules, but these modules must be installed and sealed to the SEM at manufacture stage. All SEMs require an antenna internal to the SEM/module, with an additional protected connection for an external antenna for all meter types.

6. HES Compatibility

Meters will need to interoperate with ESB's chosen HES that is implementing DLMS/COSEM to support the DLMS ACE SM GCP, as outlined in clause 6 below. A proprietary HES will not be supported.

6.1 Enhanced Meter Functions

6.1.1 Security

- The SEM will support DLMS/COSEM Security Suite 2 for messaging⁵.
- The SEM will support HLS 5 and 7 approaches for establishment of an Application Associations.
- The SEM shall be supplied with a set of unique security keys and necessary certificates pre-installed and a reasonable, secure method of transfer of these credentials to the AMI infrastructure will be agreed.
- The SEM will be capable of supporting a number of Roles including two roles dedicated to security (a "master" role and a "recovery" role), a role dedicated to operation of the Supply Control Switch, a role dedicated to configuration of the SEM, and a role dedicated to retrieving data from the SEM.
- The SEM will ensure that commands received are permitted by the role delivering the command and also that commands are authentic, not replayed and are semantically and syntactically correct before performing the command.
- The SEM will have the capability to securely change any keys or certificates present on the SEM and securely communicate the status of any security credential update to the HES. In addition, the SEM will be able to accept a change in the required security credentials via the HHT.

6.1.2 Clock and Calendar

The SEM will contain a real time clock that can display local time on the display of the SEM. The SEM will contain configurable control elements which can operate tariffs, registers, auxiliary switch, supply control switch and communication elements in response to a time occurring (both single time and repeating times). The SEM will be capable of having the clock updated as needed.

6.1.3 Tariffs

The SEM will be capable of being configured to operate a simple "24 hour" tariff, a "Standard Smart Tariff" that follows local time, and day/night tariff that follows UTC, and it must also be capable of collection of $\frac{1}{2}$ and $\frac{1}{4}$ hourly average power consumption information to facilitate a range of smart tariffs (initially $\frac{1}{2}$ hourly). The SST and other tariffs may operate the auxiliary switch(es) to facilitate the control of night storage heating or other applications. These tariffs will record relevant combinations of active import, active export, reactive import and reactive export. Status information (for example indication of power outage, clock adjustment) will be recorded within the tariff log. The

⁵ Note that meters may be configured to use some Suite 1 features for initial delivery but will be expected to be able to be reconfigured for suite 2 without firmware update.

meter will also be capable of being configured to record, deliver and reset Maximum Demand values. Values appropriate to the tariff in effect will be retained within the SEM.

6.1.4 Thin prepayment

The SEM will be capable, using a suitable security approach, of operating the supply control switch from any state into the “open” state (where supply is disconnected and can only be reconnected from the HES), the “closed” state (where supply is connected) and the “armed” state (where the supply is disconnected and can be re-connected by operation of the meter’s buttons).

The SEM will reliably communicate its Switch state to the AMI systems. For ESB, this includes the ability to transmit the relevant logical and physical state of the SEM switch so as to ensure that the state, as reflected in the AMI, is aligned to the physical state of the switch in the SEM (i.e. additional check to confirm connection state for the customer).

6.1.5 Power quality monitoring and control

The SEM will be capable of being configured to record a combination of the maximum, minimum, average and instantaneous values of voltage, frequency, THD, current, active power, reactive power and meter temperature into a log at configurable intervals to facilitate monitoring of the power network.

The SEM will be capable of being configured with a number of adjustable thresholds to permit the capture of events noting the time of excursions of these parameters beyond these maximum and minimum thresholds. The SEM shall be capable of being configured that it sends an Alert to the HES should a specific event or range of events occur.

The SEM will be capable of activating disconnection of the supply control and/or relays, if so configured based on over-voltage or under-voltage or overload conditions. Initial configuration will be such that the limiter(s) applied will generate events but will not disconnect.

6.1.6 Power Outage

The SEM shall be capable of recording an event whenever there is a power failure and whenever power is restored. These events will be capable of being sent as alert messages before the meter powers down.

6.1.7 Firmware update

The SEM will be capable of having firmware updated using a methodology that ensures that only firmware appropriate for the specific model, current version, hardware version and configuration can be activated.

Where necessary, the communications module firmware will be managed through the SEM FW update processes and return relevant information to the AMI to assess the status of any updates.

6.1.8 Event Logging and alerts

The SEM will be capable of recording events regarding all aspects of meter operations, configuration changes, and supply conditions within event logs. Other than the metrological event log, the SEM

shall be capable of configuring any event into any event log or multiple logs. The SEM shall be capable of being configured to send an alert on the occurrence of any event. This includes events and alerts configurable for security related activities (e.g. SEM key updates) and functional activities with security implications (e.g. switch status changes).

6.1.9 Routine Data Transfer

The SEM will be capable of creating a package of information and sending the package each night within a configurable time window.

6.1.10 Ad-hoc data transfer

The SEM will be capable of processing a command from an appropriate role to provide data to the requester, applying cryptographic protections (encryption, authentication and digital signature) depending on the type of data to be provided.

6.1.11 Spare Capacity

The SEM will require storage over head for an extra 25% of code space and 25% of data storage for future needs.

6.2 Integration of SEM into AMI ecosystem

Integration of the SEM into the AMI ecosystem will require SEM vendor assistance to:

- Forecast, request, and order eSIMs or SoftSIM data from the CSP (possibly via ESB networks procurement) for inclusion into the SEM during production processes.
- Engage with the HES provider to verify that the HES and SEM interact in an efficient manner
- Develop, test and deliver “flat file” data regarding the properties of meters such that ESB systems can ingest asset information in a secure manner.
- Deliver security credentials for each SEM to the HSM in a secure manner.

7. Head-End System Solution (HES)

The HES is defined within this section as all and any components and services that are required and offered by the HES Vendor that form part of their product offering. It is unlikely that vendor products will exactly align with what is described, but it is expected that the services shown will be able to be mapped into configurable and customisable deliverable components.

The following diagram illustrates the proposed HES solution

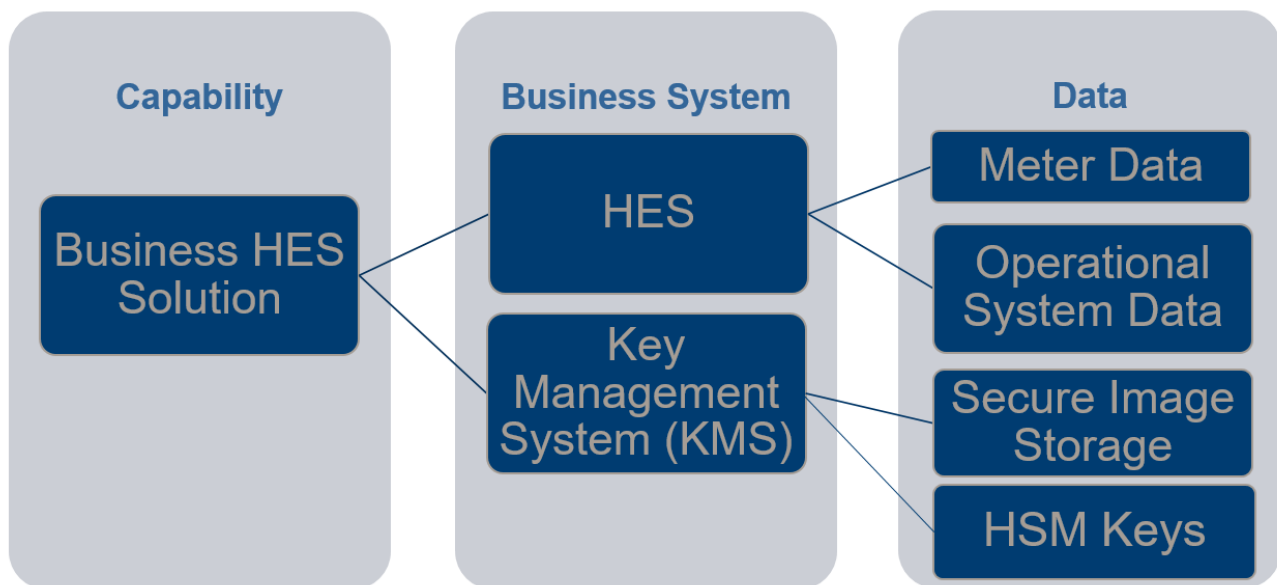


Figure 6 Conceptual diagram – HES Solution

The HES solution that is being procured by ESB contains a Head-End System and a Key Management System that work together to achieve all of the functionality required.

The HES system consists of all services that are required to manage the estate messaging to and from the SEMs and to other attached devices and AMI systems.

The KMS only interfaces with the HES and is the system that stores and maintains all data and objects that need to be secured away from the main messaging system. The cryptographic elements are stored on High Security Modules (HSMs).

As the HES and SEM use Certificate based security for some Meter Data Protocol exchanges, then the vendor should identify a Certification Authority (CA) as a sub-component of the HES. This definition of the HES includes all of the capabilities and supply of the required elements of the Key Management System (KMS) that are required to support all activities and processes described for the HES

ESB's standard operating practice for OT systems is to host these on premise. This is to satisfy the requirement to adequately isolate and recover from incidents affecting critical national infrastructure (I.e. refer NIS2).

A number of features and functions are described within the following sections to enable the HES Vendor to understand the scope, features and functions that the HES should be able to provide with limited or no development of the base product offering. Within the PQQ these are described at a high level with additional information to be provided as part of the ITT, (e.g. BPMN design, data flows and high-level test scopes).

ESB requires that the HES vendor will retain accountability for the integration of differing meter Vendor(s) and meter types for the life of the HES contract. As such the HES vendor will work with any potential SEM providers to ensure integrations are secure and aligned to the ESB smart processes that will be communicated as part of the subsequent ITT.

At the time of issuing this procurement, ESB Networks does not have any specific mandatory requirements in relation to the use of Artificial Intelligence (AI) and/or Machine Learning (ML) within the Head-End System (HES) solution. Notwithstanding this, ESB Networks recognises that the market for AI and ML technologies continues to mature, with an increasing number of relevant offerings and potential use cases emerging within the Advanced Metering Infrastructure (AMI) landscape over time.

As part of the procurement process, ESB Networks at the ITT stage may request tenderers to outline their product roadmaps, including any planned or envisaged AI and/or ML capabilities, and to describe how such capabilities could deliver future value or operational benefit over the anticipated lifecycle of the solution. In addition, at the ITT stage, ESB Networks will require the HES vendor to provide a read-only, real-time copy of relevant HES databases, or equivalent data access mechanism, that can be securely consumed by external analytics platforms and/or AI/ML systems. This capability is intended to support advanced analytics, reporting, and potential future AI/ML use cases, without impacting the operational performance or integrity of the core HES.

ESB Networks reserves the right, but is under no obligation, to consider the adoption of relevant AI and/or ML use cases during the contract term, where aligned with business needs and where demonstrable value is identified. Where an application/service contains AI capabilities and is considered an AI System under the EU AI Act, then ESB will perform an assessment on the AI System, with the support of the third-party vendor to ensure compliance with the Act. Any such adoption shall, at the point of adoption, comply with applicable legislation, industry standards and best practice, and ESB Networks' policies, governance, and information security requirements.

7.1 HES High Level Scope

The HES and KMS will, in summary, be responsible for:

- Initialisation and loading of a variety of SEMs and then management of their status across each of their individual lifecycles. Management of all attached devices including configuration, security and firmware management.
- Managing the exchange of messages and information between ESB IT systems and SEMs, over the chosen communications network(s) adjusting the messaging format and activity choreography depending on the device type, firmware and configuration.

- Monitoring, managing (including initiating, if appropriate) and reporting on all communication with the installed smart meter population in near real time. This includes managing the addressing and routing services required to facilitate communications with the installed smart meter population.
 - Creation and securing of commands to deliver the use cases in ACE SM GCP, except UC14 and UC21.
 - Proven integration with the Siemens Energy IP MDMS version V9.0 SP6 or above to support, at a minimum, the meter-to-cash use cases typical for an energy utility.
 - Support for customer devices via a local connection within the SEM.
 - Support for secure use of Hand-Held Terminals (HHT) for execution of meter commands locally at SEMs and return of data to the HES.
 - Management of security credentials used to facilitate authentication, encryption and non-repudiation of commands and data exchanged between the HES and meter devices.
- Providing access for ESB to all HES data and reporting analysis capabilities for HES and communications performance.
- Integration with the ESB Networks AMI system to support enhanced data analytics for meter performance metrics and trend analysis.
- Adjusting the performance and throughput of the HES to achieve the required SLAs on E2E functional system.
- Support of rapid diagnosis and correction of system or device operation discrepancy or failure events.
- Reporting on the operation of the SEM electricity supply switch within the SEM.
- Detailed and secured logging processes for all operations on the HES. This is particularly relevant for critical commands (i.e. meter switch operations);
- Integration with Security Monitoring tools and ESB SIEM to allow for cyber security monitoring and alerting on SEM and HES activities.
- The HES will process meter ping requests from the MDMS and manage responses from the various meter types within the agreed SLA. The primary use case for this functionality is to support ESB in recovering from large scale electricity network outages, typically during storm events.
- Operation of the P1 port in alignment with ESB processes.
- Maintaining the required performance and SLAs of HES services in the event of system or communications failures.

7.2 Key Features

ESB have described the features of the HES product as key features and, while the naming of these features may be different within the HES Vendor(s) proposed solution, offering the essence of the feature's capability should be part of the HES. Some of these features / capabilities will be detailed in later stages of the procurement process. The HES Component(s) will have the following key features as part of the product offering but not limited to the following:

7.2.1 Security and Configuration by Design

The HES should be designed with system and SEM communications security as a part of the design in a way that allows performance to be optimised to meet the required SLAs without being impacted by different levels of encryption and authorisation. The HES must be capable of supporting DLMS/COSEM Suite 2 across the whole population of SEMs.

7.2.2 Modular Structure, Operational Monitoring and Configuration

The HES should exhibit a design structure that is based in a modular service-based architecture to maximise reuse of software and allow flexibility of design and deployment to maximise systems resilience and robustness, whilst optimising the throughput of the operational system to minimise resources required and operational cost. The messaging between each module should be controlled by flexible APIs with queuing and buffering mechanisms to manage load and throughput. All aspects of the performance and operation of the HES should be capable of being monitored and controlled by operators in near real time. The structure and architecture should also support flexibility in the system to allow adjustments to interfacing, hosting etc. in the future as is likely to be required by ESB. Finally, the design should incorporate configuration of items by appropriately enabled users in preference to any requirement for coding changes.

To align with current security practices, all modules of the HES will create and forward all security alerts to the ESB SIEM system.

7.2.3 Transactional Data Store (TDS) and Reporting

The HES should be able to manage the message exchanges between the up and down stream modules and channels of the SEM, allowing and understanding if the message requires retry due to SEM availability or CSP Availability and/or queuing or buffering. The TDS should store sufficient information about these message exchanges to allow the generation of historical reports on SEM performance and processing activities at every stage. Some reports will be supplied as a part of the system procurement, but access will also be given to ESB systems to a standard data reporting application (e.g. Power BI) to all of the data held within the HES.

7.2.4 Security Application

All the Messages that are transmitted from or to the HES shall be secure so that the source and destination of the message is confirmed and that the authenticity, integrity and approval of the messages can also be confirmed. DLMS/COSEM Suite 2 will be required for messaging within an application association, with HLS5 and 7 being supported for establishment of an Application Association. ESB would anticipate that this might be achieved using certificate-based security on the message exchanges. However, other security mechanisms will be considered. It should be noted that

all data that is either transmitted or stored within the HES should not be in the clear, and that a level of security should be applied to the metadata to be transmitted. Within the AMI then, the minimum requirement is that TLS 1.3 shall be required for server-to-server transmissions and all transmissions between the HES and SEM should be authenticated and encrypted using the MDP.

The HES shall be capable of supporting all required symmetric and asymmetric cryptography. All external interfaces shall be protected in accordance with ESB policies.

7.2.5 Credential receipt and management

The HES and KMS will need to have access to the capability to protect messages in accordance with the meter data protocol from the first points of installation. As the SEM vendor will provide the relevant credentials for each meter from their manufacturing location, the HES and KMS (and/or associated system) will be capable of ingestion and storage of said credentials in a secure manner (e.g. a Hardware Security Module). If required, the vendor will support processes for the replacement/update of provided SEM credentials on first connection in a reliable and robust manner. This capability is also required to support the refresh of any security credentials that may be time limited before their expiry date (e.g. certificates).

7.2.6 Meter Messaging, Creation, routing and Validation

The HES and KMS shall be able to create, understand and translate the messages sent to the SEM or received from the SEM using DLMS/COSEM and make use of the DLMS UA ACE SM GCP, noting that security and other overarching requirements will be recorded in a SEM to HES specification document (which is under preparation). The MDP shall be capable of being transmitted directly from the HES to the SEM, but must also operate via a Hand-Held Terminal (HHT) used locally at the SEM. The MDP must ensure that the messages/responses, received either directly from the SEM or via the HHT, can be taken into the HES for processing and distribution to other components, without causing a security risk to the overall design. The HES will incorporate the capability to enforce that the messaging is always compatible to the end device which the HES is interacting with. To achieve this, the HES will be capable of loading the exact model, hardware version, software version and configuration and then mapping these onto only the valid messaging that will work with this device. When the HES updates the software and/or configuration, this update will be tracked by the HES to update the messaging that needs to be used.

7.2.7 User Interface

The HES shall have a User interface that allows authenticated and approved users to monitor, manage, maintain and understand the status of the HES and the activities and actions that the HES is responsible for. A summary of the main UI functionality required is detailed within the sections below.

7.2.7.1 WAN, HES and KMS interface Management

Management information on all of the HES interfaces and the SEM Estate will be made available for User access. Information will include the current status of connection, errors, and queue sizes in each direction along with the historical information, to be able to identify potential problems with connectivity. A messaging audit trail will also be made available for every device that has been or is connected. A user will also be able to understand any messaging issues at interfaces between HES

elements and across HES to AMI system interfaces. The HES shall be capable of reporting across various meter types and manufacturers. Management information and reporting must be available across device types so as to enable targeting redundancy and remediation activities per meter type.

7.2.7.2 Firmware, Device Configuration, and Security Credential Campaign Management

Activities relating to individual or Groups of SEMs for the downloading of firmware and activities relating to the Activation of the firmware shall be handled through campaign management functionality through the user interface. Bulk updates of devices to new configurations or with refreshed security credentials will also be carried out in a similar way, although the sequencing of an activation will not be required. It shall be possible to create, monitor, manage, pause and shut down firmware and configuration campaigns across different meter Vendor(s) and meter types

7.2.7.3 HES Status

The current status and performance of the HES component(s), together with any errors or status indicators that require action. Users will be able to view this information as a near real-time representation of system or application health.

The user may be able to alter the configuration and operation of the systems using the GUI as well.

7.2.7.4 Estate/Device Management

The estate/ device management should allow the user to understand the current operational status, settings and IDs of the SEM attached estate so that reports can be generated based on all relevant metadata that the HES is recording. This information should be able to be used as an input into firmware and or Configuration or Security credential changes that would be required throughout the life of the system. Communications will only be permitted by the HES with devices that are already known to it and that are at the required hardware, software and configuration standard.

The HES is expected to perform these functions in a SEM HW agnostic manner. This is to allow ESB to purchase SEMs from various Vendor(s) over the life of the HES. In addition, in accordance with NIS2 and other related EU level Cyber regulation the HES will support individual process per SEM type to allow for protection and update of the SEM estate in the event of an incident (e.g. isolation of particular SEMs in the estate while continuing to operate other SEMs).

Access via the GUI should also be permitted to the CSP API to allow management of CSP connectivity and SIMs.

7.2.7.5 Trend / Analytics

As part of the HES UI there should be view and reports, that detail performance trends and meter trends, that enable ESB to understand and spot potential outages in either the SEM Estate, across differing SEM Vendor(s) or the HES components.

7.2.7.6 Reporting

The HES should have a reporting suite that is accessible via the UI, with a standard set of reports that can be generated across the entire SEM estate (e.g. Install report, non-reporting firmware

version and firmware campaign reports, Configuration Reports, Operational Status reports, Performance reports, etc.). ESB require the capability for the HES to provide all data in near real time to a customer reporting environment and/or the ability to share the data with external reporting and analytics systems such as Microsoft's Power BI, Excel etc.

7.2.8 Device State

As part of the device management the HES shall be able to understand and record the state of the devices and undertaken necessary data exchanges to ensure that the HES and Device are in sync. (e.g. Created, Installed, Assigned, De-installed, Testing, etc.). It shall also be able to report on these states and the historical changes in state per SEM type. The state model for the attached devices will include states where communication is suppressed due to security issues with the device and its hardware, firmware and configuration status. The state will be updated and maintained after every communication with the device.

7.2.9 Event Management

The HES shall create notifications based on the operation of ESB Business Processes along with events generated due to the devices and/or messages that it processes. These notifications shall be used via the OSS and other AMI systems to understand the current SEM performance (i.e. including comparative reporting between SEM types) and HES Performance. The HES shall be able to present any of this to the HES User for analysis and understanding, via UI, reports and APIs.

All security events will be forwarded to the ESB SIEM environment for analysis and capture. These events should be unique and identify the relevant SEM type to allow for the detailed assessment of potential threats and mitigation based on a particular SEM type.

7.2.10 Device Configuration and Firmware / Configuration Campaign Management

The HES shall be able to be configured with support for many variations of attached devices with differing hardware, software and configuration. The HES will only permit the loading of device inventory where this aligns with the list of devices that are supported by the system. The HES will also be able to be configured so that only validated upgrade paths for firmware and configuration can only be set up as campaigns. In addition, the HES configuration will ensure that message formats and communications are always compatible with the attached devices.

The HES shall be able to manage the configuration of the Device in line with the features of the AMI System, i.e. SDC, DTC and DMC. It shall also be operating firmware campaigns and possibly act as a store for the approved version and previous versions for multiple types of devices. As such the HES is expected to be able to create campaigns for all types of firmware updates and configuration updates called out within the previous sections of this document. There shall be a User Interface for the campaign management and a standard set of reports that can be generated.

7.3 HES System Use Cases

7.3.1 High Level Use Cases

The following table lists some of the many use cases within ESB that involve HES operation requirements and processes. This list may be amended at any time but is included here in order for

Vendor(s) to understand some of the scope of the requirements. Throughout the lifespan of the HES, these use cases will be added to or amended and applied across many different SEM types.

Table 5 – HES Technical Use Cases

#	Feature	HES Technical Use Case (TUC) Description
1	Device Lifecycle	SEM Provisioning process (shipment file)
		SEM discovery / registration
		SEM installation process
		SEM Deinstallation process
		SEM Exchange process
		SEM Manual Scrapping process
2	Data Collection	Data collect (push mode)
		On Demand Read
		Event collection and processing
		Meter alarm processing in HES
3	Device Operation Management from the HES	HES feature to manage FW upload in the HES library
		HES feature to create FW campaign
		HES feature to download FW download
		HES feature to activate FW campaign
		MDMS requires to retrieve the firmware version from the SEM
		Time synchronisation process between HES and SEM
		HES feature to manage HES DTC campaign (Expert COSEM)
		HES feature to manage key renewal campaign
4	Device Operation Management from MDMS	Configure SEM (outside standard provisioning and commissioning process)
		Configure SEM (outside standard provisioning and commissioning process)
		MDM to trigger the Connect / Disconnect (CDC) Check status
		MDM to trigger a connect request
		MDM to trigger a disconnect request

#	Feature	HES Technical Use Case (TUC) Description
5	Device Communication	HES Connection establishment process (PULL) and SEM Connection establishment process (PUSH)
		SEM process to connect to WAN
6	Monitoring	HES feature to manage report
		HES feature to manage the monitoring dashboards
		HES feature to manage the monitoring of P2P meters communication
7	HES Limiter Configuration	HES feature to update the meter switch limiters configuration
		HES feature to reset the meter switch limiters counters

These use cases will be mapped to the ACE SM GCP Use Cases and HES operations as a part of the of the ITT.

7.3.2 Creation and Install, Removal and Swap out

One of the ESB meter management key activities is that of the creation and set up of the device within the systems and HES. The HES shall be capable to enable the device to operate within the Estate and authorise communications to flow from the upstream AMI System. As part of the install, should it be required, the HES shall be able to manage the installation of the SEM without upstream interactions. The HES shall be able to work within the key factors of ESB install and provisioning process:

- **Zero Touch installation:** Limited to zero interaction is required by the SEM at installation to ensure that installer time on site is limited to the electrical installation of the Device, with limited to no requirement for contact with ESB Operations teams for device commissioning.
- **Siemens Provisioning Process;** see the MDMS adaptor section

The HES shall also support the provision of new endpoints and metering on these, swap outs of one meter for another (agnostic of meter vendor or type), and meter and endpoint removals.

7.3.3 Switch Operations

The Meter + solution will support the use of the SEM supply control switch for use either as part of thin prepayment that is offered by the suppliers within Ireland or as value added service to credit energy consumers. Therefore, the HES shall be able to accept, process and reply to connection and disconnection messages for a SEM(s).

Support the provision of identified SEM events and alarms on switch status verification to ensure the alignment of the physical and logical state of the switch (i.e. supplementary process to confirm meter switch state is as expected by the market).

Support the implementation and report in the activation of various controls around the volumes of switch operations allowed in a period (i.e. Throttling).

Support the execution of any remediation activities initiated as part of switch related incident management process to enable the operation of the switch in an emergency.

Integration with Security Monitoring tools and ESB SIEM to allow for cyber security monitoring and alerting on SEM and HES activities.

7.3.4 Meter Ping

The HES will process meter ping requests from the MDMS and manage responses from the various meter types. The primary use case for this functionality is to support ESB in recovering from large scale electricity network outages, typically during storm events.

Note: Meter Ping is a term used in ESB to describe the basic ping, and also on-demand read of registers and profiles. The returned message may also include other relevant data that will need to be stored in the HES.

7.3.5 Last Gasp (LG)

The HES shall support the capability within the SEM to configure (through Remote COSEM campaign) the Last Gasp capability that will push a LG notification to the HES. This is to include the enablement of additional events on both single and three-phase, WC and CT SEMs. On receipt of the Last Gasp Notification from the SEM the HES will initiate an alert and push on to the MDMS. MDMS may export those alerts and other power outage related events to an ESBN System (NetOps).

7.3.6 P1 Port

The ability for the HES to receive and validate the following individual requests from the MDMS:

- Disable/ enable encryption of a P1 port.
- Enablement of a P1 port.
- Disablement of a P1 port.

7.4 HES System Interface Overview

The diagram below shows the context of the HES solution and the connectivity and context within the ESB environment.

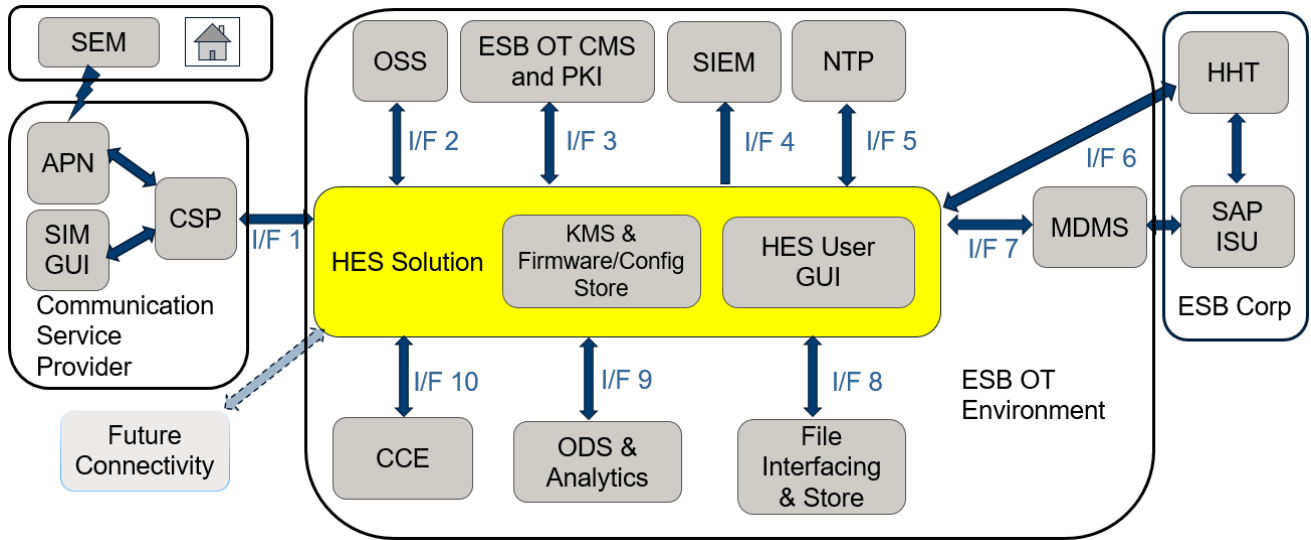


Figure 7 HES System Context and HES Interface Diagram

Table 6 – AMI System Context Overview

Location	Component	Component Description
ESB Corp	ESB SAP IS-U	ESB SAP Industry Specific Solution for Utilities
	ESB HHT (I/F 6)	ESB are working on integrating HHT with the Meter. An interface is required from the HHT to the HES.
ESB OT Environment	ESB OT File Interfacing (I/F 8)	The ESB OT File Interfacing is a set of Secure Services that allow for the transfer of files between ESB Corp and ESB OT environments.
	ESB OT File store (I/F 8)	The ESB OT File Store is a number of secure file locations within the OT environment that can be used to store reports and data, required by the AMI Applications or to be sent to the Corp systems for consumption and analysis.
	ESB OT CMS and PKI (I/F 3)	The ESB Credential Management System (CMS) will be used to align the HES user structure with that of ESB. The PKI Certificate Authority Service for IT is used for the creation and management of digital certificates used within the OT environment to secure internal OT system to system access. The vendor should not assume that this can be used for MDP security requirements. All ESB Users shall use 2FA.
	HES Solution KMS & Firmware/Configuration Store	This is the set of Security Applications that may include HSM, CA and other applications and devices that the vendor may provide to ensure that the communications between the HES and the Device Estate is secured within the MDP (Meter Data Protocol).
	MDMS (I/F 8)	This is the existing MDMS (Siemens EnergyIP) The HES selected during this procurement must interface to this MDMS.
	Operational Data Store & Analytics (I/F 9)	The Operational Data Store & Analytics (ODSA) system is a number of applications, data bases and tools, that ESB utilise to provide additional services to the ESB User Estate.
	ESB Operational Support Systems (OSS) (I/F 2)	The ESB Operational Support Systems (OSS) is a suite of software used to manage infrastructure, systems and networks. This includes MS SCOM, AV and other such applications that are base support systems for any data centre environment.
	ESB SIEM Security Monitoring (I/F 4)	This is the one-way feed of security events into the ESB SIEM system for analysis and reporting
	CTF (I/F 10)	This is an interface to the CTF system where communications levels can be extracted and used by the HES and data can fed to the system to enhance the reliability and accuracy of the calculation

Location	Component	Component Description
	HES Solution User GUI	This is the GUI interface that HES and KMS users will operate the system over
	ESB OT NTP (I/F 5)	The ESB OT NTP server is used to set the correct time of the OT environment.
Communication Service Provider (I/F 1)	SIM Management System (I/F 1)	The SIM Management System is the CSP's service and platform for the management of the eSIM Estate.
	APN (I/F 1)	An Access Point Name (APN) is the name of a gateway between an MNO and another computer network.

It is also likely that additional interfaces will be required over the lifetime of the HES solution.

7.5 HES High-Level Service Components

The HES shall have several functions that it shall undertake in conjunction with the KMS that have been defined within the previous section. Within this section of the document the view is more on the architecture of the HES and the requirements to ensure that the HES can communicate with other systems and components of the AMI solution.

The HES has for this reason been described as several key services that allow ESB to describe the overall requirements of the HES. While this is ESB's view it is not prescriptive in the HES Design or implementation.

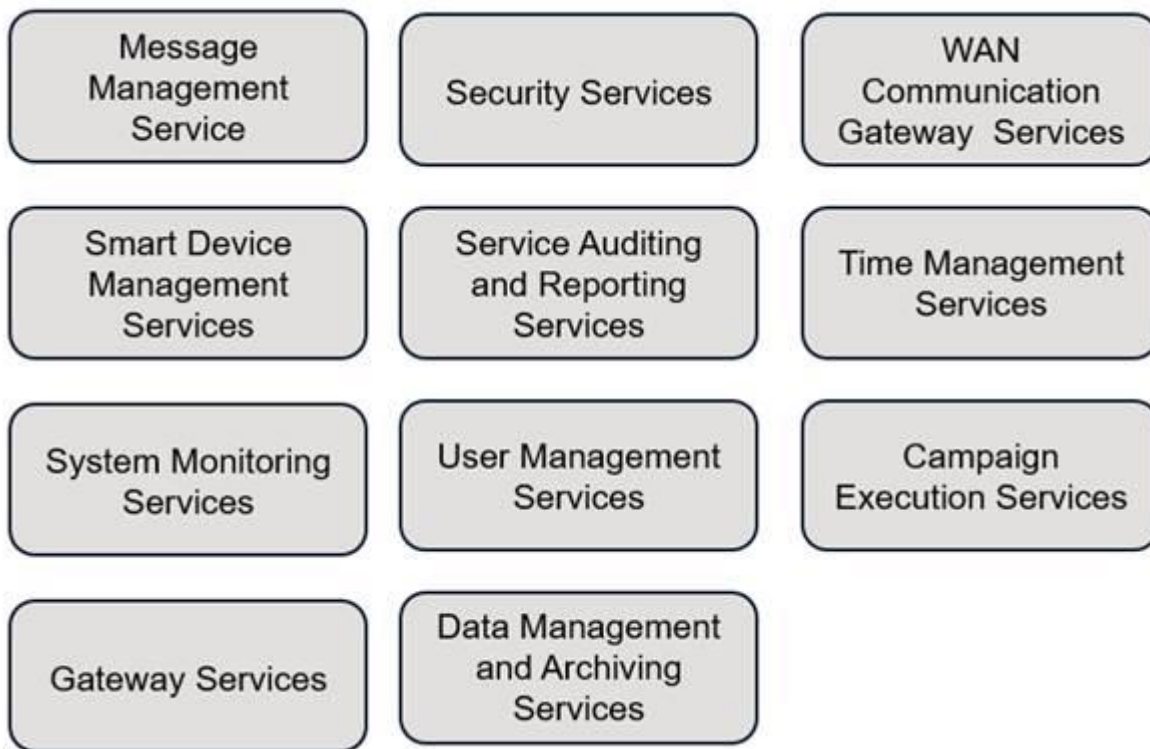


Figure 8 HES High Level Subcomponents

7.5.1 Message Management Services

The Message Management Component deals with the core routing and translation of incoming messages from the CSP that connects the SEM to the Head-End System. It also deals with the routing of the data between the HES and the other AMI System components.

The following are anticipated lower-level services within this component:

- Message Orchestration
- Processing Business Service Requests
- Message Translation
- Message Routing Engine
- Manual Message Triggering
- HHT Operations
- Message Queue Management System
- Message Throttling and Prioritisation
- Exception Handling

7.5.2 HES Security Services

The HES shall provide security services to protect all cryptographic operations and security-critical functions. These services shall enforce message integrity, authentication, non-repudiation and device-level security controls in accordance with the SEM to HES specification.

This is the HES capability to secure every message that is passed to and from the WAN with the appropriate encryption and signature, and to correctly decrypt, validate the signature and translate

any response or any other event or alert. Each message is secured by the required cryptographic credentials (symmetric keys or digital certificates and associated private keys) associated with the individual SEMs and manage the replacement of this over time. Depending on the cryptographic model deployed this will involve integrating with the KMS for SEM Certificate updates. The HES will allow authorised users to track the cryptographic credentials in use and manage their replacement on SEMs.

Only messages that require signing with private keys or validating with public certificates will be forwarded to the KMS for action.

The following are anticipated lower-level services within this component:

- HES Security Credential Management
- Security Incident and Event Management Services
- Cryptographic Operations Service
- Message Threshold and Anomaly Detection
- Event Management Service
- Anti-Replay
- Role Based Access Controls

7.5.3 Auditing

This is the HES capability to log all transactions and the services required to allow them to be reported on without impacting the performance of the HES.

The following are anticipated lower-level services within this component:

- Transaction Logging
- Reporting and Querying
- Security logging

7.5.4 WAN Communication Gateway Services

The WAN interface requires a set of services that are greater than and different from the other gateways. It includes the handling of communication problems on the WAN as well as providing the throttling of messages to devices where this may lead to a security problem.

The Services also include protection of the HES of deliberate or non-deliberate DoS attacks such as Alert Storms.

The following are anticipated lower-level services within this component:

- Message Handling Service
- Event Handling Service
- CSP and SIM management Services
- Message Audit trail service
- Service Auditing and Reporting Services
- Security Protection Services
- Authentication Services
- Smart Device Communications

7.5.5 Smart Device Management Services

These services manage all of the data associated with managing and changing the device information and statuses based on the transactions that occur within the HES. Initial data is loaded from files.

The following are anticipated lower-level services within this component:

- Smart Device Data Management
- Smart Device Status Management

7.5.6 Service Auditing and Reporting Services

The HES shall provide service auditing and reporting services to support access by authorised external reporting and data analysis tools. These services shall allow controlled access to audit and reporting data while protecting sensitive cryptographic material.

Only metadata required to access services provided by the HSM and Firmware Store shall be exposed.

The following are anticipated lower-level services within this component:

- Device Reporting
- System Reporting
- Service Reporting
- General Reporting
- Reporting data to ODS and OMR

7.5.7 System Monitoring and Management Services

The HES shall manage all of the interfaces that it provides and ensure that appropriate measures are implemented to ensure that the smooth operations of the HES within the AMI system is monitored and managed to minimise outages or errors and maintain compliance with all availability and performance SLAs.

The following are anticipated lower-level services within this component:

- SLA monitoring Services
- HES System Event and Alert Service
- Automatic resource allocation services
- File Upload
- Management Interface

7.5.8 Time Management

The HES shall provide time management services to ensure consistent time synchronisation across the system. System time shall be aligned with the ESB enterprise time source.

The following are anticipated lower-level services within this component:

- HES Time Synchronisation
- Meter Time Clock Synchronisation

7.5.9 User Management Services

This is the management of all of the services that are available to HES UI users.

The following are anticipated lower-level services within this component:

- HES User Security Services
- HES monitoring service
- Management Services
- Manual SEM monitoring and Message services
- Manage and load SEM information
- File import services
- File export services

7.5.10 HES Campaign Management and Execution Services

This service allows UI users to create, initiate, manage, monitor, and control campaigns for firmware, configuration, and security updates on the attached device population.

This service will automatically execute the campaigns that have been set up by users in priority order and in accordance with the level to which the system will allow, in order to maintain compliance with the service SLAs.

7.5.11 Gateway Services

The HES shall manage all of the interfaces that it provides and ensure that appropriate measures are implemented to ensure that the smooth operations of the HES within the AMI system is monitored and managed to reduce outages or errors.

The following are anticipated lower-level services within this component:

- Security Protection Service
- Queueing Service
- Logging Service

7.5.12 Data Management and Archiving Services

This service maintains the integrity and performance of all data in the HES system.

It also moves data offline and archives any data that is stale in accordance with ESB policies and the functional reporting requirements.

7.6 KMS High-Level Service Components

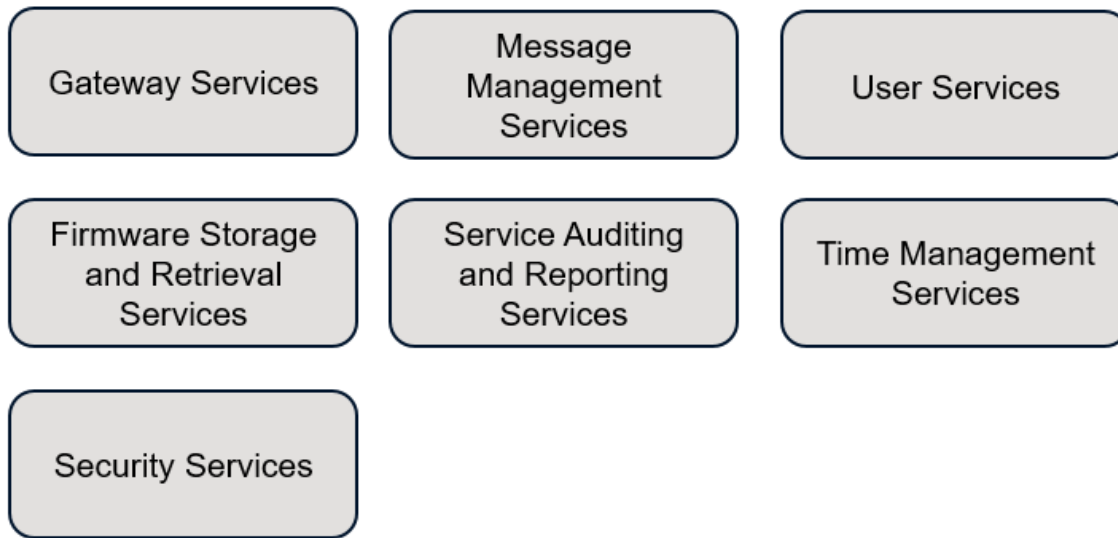


Figure 9 HES High Level Service Components

The Key Management Service is the component within the AMI system which maintains the lifecycle of all device credentials for the Device Estate. It also could be used to store and manage the Firmware and configuration management libraries.

Figure 9 above gives a conceptual view of the key services or features of the KMS to assist the tenderer in understanding the requirements that ESB have in relation to the security management of the AMI System to be provided.

7.6.1 Gateway Services

This service is required for every interface that carries data using restful messaging technologies. On all of these interfaces, the connectivity must be constantly monitored and managed to deal with any issues using buffering and retries where necessary.

The following are anticipated lower-level services within this component:

- Security Protection Service
- Queueing Service
- Physical Connection Switching Service
- Logging Service

7.6.2 Message Management Services

This service manages the messages that transition between all of the elements in the KMS including to and from the gateway.

The following are anticipated lower-level services within this component:

- Queue Management Services

- Message Queue Prioritisation Services
- Encryption and Decryption Management Service
- Message Logging and Reporting

7.6.3 User and Access Management Services

The KMS is required to be a high security component in the AMI solution. The KMS shall ensure robust user profiles are applied and that these are supported with detailed secure logging so that all access to the KMS can be audited and investigated.

This Service manages the users access and permissions across all of the KMS. It interfaces with the main Active Directory capability and structure in AMI Systems.

The following are anticipated lower-level services within this component:

- User Management and Permissions
- KMS service monitoring

7.6.4 Firmware and Configuration Storage and Retrieval Services

These services cover the capability of the KMS to securely store the firmware and configuration images that are available to be loaded onto the SEMs. These images are to be securely signed by the manufactures factory.

The configuration images will include a range of configuration changes from a full set of all items through to individual changes, (example would be enabling or disabling the P1 port).

The following are anticipated lower-level services within this component:

- Firmware and Device Configuration Loading Service.
- Key and Certificate Management Service.

7.6.5 Service Auditing and Reporting Services

This service is similar to that of the HES as it will allow external reporting and data analysis tools access to all data within the KMS.

The exception will be that only the metadata used to access the services in the HSM, and the Firmware Store will be accessible.

7.6.6 Time Management Service

This service will be the ability of the KMS to maintain all times in the system to align with the main ESB NTP service.

7.6.7 Security Services

The KMS must maintain the security of its services using a number of functions.

The following are anticipated lower-level services within this component:



- Message Signature, encryption and Anti-Replay Verification
- Event Management Service
- Key Generation and Storage
- Encryption and Decryption Management
- Message Signature Generation and verification
- Device Recovery Support

8. Non-Functional Requirements Overview

8.1 Security

Security of messaging and infrastructure is an important element of the HES together with the integrity of all the message tunnels, queues, user privileges and activity.

All security features will be described in a security plan and architecture document that is approved by ESB before implementation.

ESB Security Policy must be aligned with at all times.

8.1.1 Message Security

The HES shall support configurable message security aligned with SEM security requirements. This shall include support for multiple DLMS security roles and configurable security levels applied per message type and use case.

Message security shall support encrypted tunnelling, symmetric and asymmetric encryption, and symmetric and asymmetric signing. Cryptographic keys and certificates shall be securely stored within HSMs managed by the KMS. The HES will have the capability to update security credentials.

8.1.2 SEM Use Case Security

The HES shall support assignment of security levels to SEM use cases. Security levels shall be configurable based on device attributes including manufacturer, model, hardware version, firmware version and configuration. All configuration of use-case security shall be performed by suitably authorised users via the HES UI.

It should be possible to support different security levels across a matrix of use cases for different devices, based on manufacturer, make, model, hardware version, firmware version, and configuration. All such flexibility must be configurable by suitably privileged users through the HES user interface.

8.1.3 Gateway Security

The HES should ensure that all gateways are protected using encrypted communication channels. Where gateways connect systems in different security zones, messages should also be signed and validated in each direction.

All gateways will be secured with encrypted tunnels between each element where they are connected within the same security zone. Where systems are not in the same security zone, then all messages are also signed and validated in each direction. The CSP Gateway will also contain additional security and attack resilience capability.

8.1.4 KMS Security

The KMS shall be deployed in a manner that ensures the protection and portability of cryptographic credentials. Hosting on ESB premises is required, with support for deployment in microservices environment where required.

8.1.5 Data Security

All data shall be protected in accordance with ESB policies and processes. Data subject to GDPR requirements shall be encrypted at rest and in transit.

8.2 Service Availability and Disaster Recovery

The HES must be a high integrity and high availability system, although the availability and integrity can vary by service type and use case. ESB does not expect service availability to be impacted by any system maintenance requirements, and the implementation of the HES and KMS should support this requirement.

The HES shall meet agreed availability, Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets and the actual service levels achieved will be reported on a monthly basis.

The HES system must be designed and implemented in a manner that not only supports the availability and recovery times, but also to be capable of supporting these requirements in the event of significant failures of infrastructure and other potential disasters.

Backup and restore policies procedures and operations must be put in place for all data, systems and configurations to support these requirements. ESB will need to regularly prove the Disaster Recovery plan of the implementation for each service.

Special processes and procedures must also be in place to back up the contents of HSM to ensure that no cryptographic material will be lost under any circumstances. The design and implementation of the HES system must be supported by a Failure Mode, Effect and Criticality Analysis document that must be delivered to ESB for approval before implementation.

8.2.1 Data integrity and Backup

Processes and procedures must be put in place to ensure that all operational data is maintained to support the required integrity and content replication between systems. The data contained within the HES and KMS must be maintained and supported in alignment with the configurable Data Retention and Backup Policy.

Particular attention should be made to the retained meter readings where replication to the MDMS is required. Whilst the quantity of the readings will be limited in the HES, all values must be passed to the MDMS and held there.

Power Quality readings will all be held in the HES database and synchronised with other ESB reporting systems for reporting to the business. Synchronisation of data between HES/KMS, the MDMS and other systems must also be supported.

All Events, Alerts and any data associated with device communication will need to be retained within the HES to support the investigation of meter issues. The Data Retention and Backup Policy will detail how and when meter audit trails will need to be archived or sent to offline storage and the system design must support this in a controlled manner.

8.3 Performance and scalability

The HES will be designed in a modular functional manner. Services should be distributed using containerisation (or equivalent) wherever scalability is required. Scalability should be provided based on manual, scheduled or dynamic instantiation or destruction of new containers and services within the dynamic environment. At no point should any data or services be lost during this scale in and scale out processes.

The modular nature of the HES design should cover scalability and resilience to failures to maintain the required availability targets. The end-to-end performance of the HES and KMS will constantly be monitored and adjusted to align with the defined SLAs. The SLAs agreed with the Vendor will include at least the times taken across the HES for both requests and responses and also the response times for device estate and ESB system service requests. The SLAs will vary by use case and service request and include a data accuracy measurement as well as timings. These will be covered in more detail in ITT stage.

The HES should be as linearly scalable as possible, based on the number of containers deployed within each service area of the system. The HES must be right sized at all times through appropriate resource controls and measures. The system should support scalability over short- and medium-term timescales.

8.3.1 Infrastructure Requirements

All HES systems must comply with the ESB OT infrastructure policies. The HES monitoring screens will need to provide accurate and near real time performance and alerting updates to allow users to activate recovery processes immediately.

As a part of these services, both event production and status monitoring of the infrastructure will also be required. The availability and recovery times for these elements must be included in the overall system availability calculations. As described above infrastructure events and alerts must be communicated to the HES/KMS support and security systems to allow compliance with availability, performance and security SLAs.

8.3.2 Design Flexibility

The system shall be designed in a manner that permits adding, reconfiguring or eliminating communication channels or ports using configuration rather than reprogramming. For example, it may be necessary to increase or amend the number of connections to the CSP(s), and these changes should be achievable with little or no effort and through configuration only.

Additional or amended functionality within system components should be introduced in a manner that does not impact existing services or connections, thereby minimising the need for regression testing and simplifying deployment. For example, the introduction of a new meter use case into the system

should be carried out and implemented without impacting existing functionality and deployed into live operation with no impact on system availability.

In a similar manner to the above, it is likely that more complex cryptographic algorithms will need to be applied to the system to counter quantum computing threats. Whilst this will involve amendments to software, this should be able to be configured into operation on the HES/KMS as an additional function rather than reprogramming of a large part of the software.

8.3.3 Technologies used

The technologies employed in the design, construction, and deployment of the system should support the efficient development of microservice-based modules and classes that can be containerised, together with SQL and non-SQL databases and other complementary technologies suitable for operation in both private cloud and on-premise/local environments.

It is strongly preferred that community-supported, freely accessible technologies are used rather than proprietary alternatives, and that system elements and deployments can be moved seamlessly between private cloud and on-premise/local environments to maintain flexibility throughout the system's operational lifecycle.

8.4 System Acceptance and ESB Environments

8.4.1 System Acceptance

The system acceptance processes will be carried out in accordance with ESB processes. Both functional and non-functional requirements must be demonstrated.

Acceptance criteria will be tested against the requirements of at least:

- End to End use cases
- All interface specifications
- Design Specifications delivered by vendor and assured by ESB
- Interfaces must be in accordance with the Design Baseline documentation
- Other relevant Design Baseline documentation

8.4.2 Feature Development and Acceptance

As part of the operational life of the AMI Systems and the HES there will be a need to create new features for the HES and the Devices, therefore, the control for the creation of configuration changes should be under the control of ESB, with advice from the HES Vendor. Should the Feature require new SW or firmware or configuration for either the HES or the SEM, ESB shall be able to request development through the ESB Change control process.

8.4.3 ESB and Supplier Environments

The ESB Environments are based on either the Testing of the system and solution or used for training. As such the training environment shall be the same as the production environment and shall be a standalone environment for ESB to use to train internal staff on how to use the System.

In order to minimise development cost and risk, methods such as “Infrastructure as Software” should be available so that test environments can be created or edited at low risk at any time to support the different test stages and system capabilities at a particular point in the development and testing. Test environments should be able to be removed and restored, scaled in and scaled out, at any time to minimise operational cost.

ESB expect that the chosen HES Vendor and CSP shall be able to operate within their own control environment that allows the Vendor(s) to develop, test, verify and demonstrate any releases to ESB either as part of operational life or project stages before transfer to any ESB systems. It is expected that the vendor will have test regression packs available for these activities and that these shall be automated to reduce cost and risk.

8.5 Release Management

ESB shall release each of the stages into the production environment post the validation of the functionality through the testing process. Therefore, there is a need to have sufficient environments to enable the active release plan and detailed release notes.

8.6 Software Releases and Maintenance

As the HES/KMS is a set of software components created to deliver a set of features. ESB expect that over the life of the system some of these software components will require updates to the base OS or applications, or because of new features or functions of the Product.

There will be a continuous stream of maintenance releases to the product and its supporting software and infrastructure. This shall be supported by the Vendor(s) long-term roadmap.

As a part of the initial system delivery, the supplier will include a software configuration and maintenance plan that will be agreed with ESB. This will include the details as to how the configuration of the HES/KMS will be maintained and delivered as well as the processes and authorities around these deliveries. Each updated delivery will include a Change Note that specifies the impact of the changes, configuration and functional/non-functional impacts. A full bill of materials should be maintained at all times. These change proposals and notes will need to be agreed with the change control process by ESB, before being approved into any maintenance schedule. The agreement with ESB will also include a testing path into production, utilising one or more testing environments.

All documentation must be maintained alongside the system components and delivered as a part of the change process.

9. Home Area Network (HAN)

9.1 Overview

This section is retained for reference.

- In this procurement, HAN management is limited to the enablement and disablement of the P1 port required on the meter, configuration of the data items published on the port, and enablement and disablement of encryption on the port. To support this, the HES (and SEM) will use the data structures within the ACE SM GCP, noting UC20 (for the security aspects) and UC12 (for the other aspects).

10. Integration and development of an Adaptor to the Siemens Energy IP/Gridscale⁶ Meter Data Management System (MDMS)

Integration and development of an Adapter to the Siemens Energy IP/Gridscale¹ Meter Data Management System (MDMS)

10.1 Overview

The Integration and development of an Adapter to the Siemens Energy IP MDMS will in summary be capable of receiving, processing and acknowledging of data, readings and associated events and alerts from connected SEMs located within the Republic of Ireland. It is the responsibility of the HES provider to track and maintain the adapter integrating to Siemens EnergyIP MDMS and all subsequent releases of the MDMS. This interface must meet the IEC 61968-9 standard.

It is envisaged that the Adapter to the Siemens EnergyIP MDMS will be used for at least the following functionalities:

- Proven integration with the proposed HES to support the meter-to-cash use cases typical for an energy utility.
- Receipt of events and alerts from the HES into the MDMS.
- Meter Firmware version visibility to the MDMS.
- Support for ad-hoc data requests from MDMS down to the meter for all supported metrologies.
- Delivery of all consumption data from the HES collection process to the MDMS through this adapter. This must include the post-midnight data push of final HH intervals and register reads across the whole portfolio within a three-hour window to fulfil the ESB Networks market obligations.
- Support for ESB E2E use cases and services (CoS, CoLE, Remote Switch Operation Requests, Change of Tariff Configuration, Enablement/Disablement of P1 Port).
- Meter installation, meter exchange and meter removal, requiring the registration, provisioning and update of the meter data between the HES and MDMS.
- Meter switch operations (remote connection/disconnection) related market offerings and processes requiring the operation of the meter switch (e.g. thin prepayment services, Non-Payment of Account (NPA) etc.)

⁶ The EnergyIP MDM is rebranded Gridscale from version 9.1 onwards.

- Operation of the P1 port in alignment with ESB processes.
- Processing of last gasp events and alerts.
- Support the remote enablement/disablement of In-Home Channel (IHC) to support the customers self-provided In Home Display (IHD).
- Processing of last gasp events and alerts.
- Support the remote enablement/disablement of In-Home Channel (IHC) to support the customers self-provided In Home Display (IHD).

The main features of the integration between the Tenderer's solution and the Siemens MDMS include a set of adapter features as described below. These may be added to or removed as a part of ongoing changes required to support the ESB business. Since this interface is to a standard, the vendor should be able to carry out with little or no impact to system design or operation using configuration amendments that will preferably be able to be carried out by ESB staff as a part of the HES product support scope.

10.2 Meter Reading

The Adapter's Inbound Read service will enable the transfer of the consumption data (half hourly intervals of Power and midnight snapshot of Energy registers) transmitted from the meters to the HES, through the Adapter and into the MDMS. The push of this consumption data post-midnight (all meters must push the previous day's consumption data by latest 2am) must be transferred across to the MDMS by 3am and therefore this is a key feature of this interface. It is down to the Tenderer working with Siemens to provide an adapter to support the data metrics based on the HES supported device estate.

10.3 Events

The HES will receive event logs from the meters and filter the required events that require forwarding to the MDMS. The Adapter's Inbound Event service must ensure timely processing aligned to the Read processing.

10.4 Provisioning

The Tenderer's solution will enable provisioning for newly installed meters, ensuring the data model of the meter to site is created, maintained and ended as required through adapter services initiated from the MDMS to the HES. Throughout, the MDMS should be able to confirm the current status of the meter and have responses provided to requests across the Adapter to confirm outcomes.

10.5 Switch Operations

The Meter+ solution will enable the use of the SEM supply control switch for use either as part of thin Prepayment that is offered by the suppliers within Ireland or as value added service to credit energy consumers. Therefore, the Adapter shall support the accept, process and reply to disconnection/connection messages for a meter within the agreed SLA.

In parallel, the Adapter shall support the processing of meter events and alarms related to the switch status verification to ensure the alignment of the physical and logical state of the switch (i.e. supplementary process to confirm meter switch state is as expected by the market).

Throttling controls to restrict the number of connections; and independently disconnections in a configurable period, are required to be set at adapter level requiring the Adapter to be tightly integrated to the MDMS capability.

A remote SCS (Supply Control Switch) Status Check service available through the MDMS Adapter will provide On Demand or Meter Ping initiated use cases with a mechanism to check the status of the meter's SCS.

10.6 On Demand Read / Meter Ping

The MDMS and upstream components will require ad-hoc information from the meter. Therefore, the MDMS will request via the On Demand Read service the HES to create a request to the meter to be able to read data and return it to the MDMS. There are several automated use cases that relate to E2E business processes (e.g. CoLE, CoS) that utilise this.

As well as these core business use cases, there is also an ESB capability that supports ad hoc trigger including en masse: Meter Ping. This is an ESB AMI capability that utilises the same services in the Adapter as the On Demand Reads to allow Meter Ping requests to be made to a meter for data (e.g. measurements, instrumentation data, SCA status check) to be retrieved back. The primary use case for this functionality is to support ESB in recovering from large scale electricity network outages, typically during storm events, identifying availability of service across the portfolio/network. The above terminology is specific to the AMI system within Ireland.

10.7 Alerts and Last Gasp

Processing of Alerts including Last Gasp information from all the HES(s). ESB currently use Alerts for limited scenarios, notably SCS operations and Last Gasp. Use is likely to expand to other applications (e.g. voltage level, phase imbalances, etc). Prompt and reliable delivery of these messages can be essential to some activities (e.g. thin prepayment depends on the alert to confirm SCS state after disconnection/reconnection operations).

10.8 P1 Port

The Tenderer's solution will support the ability for the MDMS to request and receive a response to/from the HES for the following individual requests that support the enablement of the IHC to enable customers IHDs:

- Disable/ enable encryption of a P1 port.
- Enablement of a P1 port.
- Disablement of a P1 port.

10.9 Smart Device Configuration

The HES shall be able to accept requests from the MDMS to change the configuration of the meter via the Set Meter Configuration services. This can include but is not limited to, Push Configuration, Measurement Recording Configuration (e.g. configure specific registers to record in alignment to an MCC02 configuration rather than MCC16), Meter Display and Aux Switch.

In response, the HES must provide confirmation via the Adapter of the outcome of the change in configuration and if requested via the Get Meter Configuration, provide a suitable view of the confirmed configuration that has been applied to that meter, likely through an agreed profile that represents a particular configuration.

10.10 Firmware

The Adapter will provide the option for retrieval by request from the MDMS, of the applied version of firmware on an individual meter. This is likely to be part of the Get Meter Configuration.

10.11 Summary of Performance

The Adapter between the MDMS and HES shall be able to support the processing of the Billing sets for minimum of 2 million SEM's within 2hrs with the option to be scalable, the quantity of messages is down to the implementation of the AMI Vendors design. It is envisaged that this may scale to 3 million. This is in addition to other normal operations that shall be undertaken within the AMI system. It should be noted that CoS and CoLE will normally be undertaken at 00:00:00.000 by the SEM / System and it is currently assumed that between 10 and 20% of the estate could undertake this activity per night.

10.12 Integration of the MDMS Adapter

ESB expects that the Tenderer will be responsible for providing the required resource and technical capability to integrate their solution offering to the Siemens MDMS. It is expected that this integration is already complete against IEC 61968-9, and this will be a condition of the award. It is not acceptable for the AMI Vendor to assume that the design build and test of a new MDMS adapter can be undertaken within the project time scales, minor enhancements to an existing adapter maybe acceptable within the project time scales.

Further, the standard product provided by Siemens includes the UAA Adapter. This is currently utilised by ESB and therefore aligns to the E2E design and is the preferable Adapter to maintain consistent, Siemens assured integration between the core MDMS processing and the ESB Head-End Systems.

ESB expect that the support for the MDMS adapter should contain all necessary licence, integration, and uplift cost for the Siemens MDMS Adapter to support a minimum of 2 million devices are the responsibility of the AMI Vendor and should be clearly identifiable within the solution offering. It is envisaged that this may scale to 3 million.

11. Communications Service Provider (CSP)

The CSP, 3Ireland delivers communications service interfaced to ESB IT systems and SEMs meeting the coverage, reliability and performance SLAs, to support SEMs installed in the Republic of Ireland. For clarity, ESB Networks are not procuring communications services in this process.

11.1 CSP Scope

The high-level scope of the communications service provision is outlined within the following sections.

11.1.1 Communication service between ESB IT systems and SEMs

The CSP opens and manages communication links with authenticated SEMs via the WAN interface initiated by either an ESB IT system or by a SEM for the secure transport of MDP data over these links using standard protocols. SEMs that attempt to join the network are authenticated using SIM credentials, and against devices that have been Whitelisted⁷ and not subsequently Blacklisted⁸ by ESB using the communication service User Interface or an Application Programming Interface (API); and all data sent to and from SEMs is required to be encrypted.

11.1.2 Communication configuration

Where any item of equipment in the solution requires a SIM to connect to the mobile network, including the communication interface embedded in each SEM provisioned by the AMI Technology Provider, the Communication Provider will provide eSIMs or provisioning capability for SoftSIMs.

SIMs for SEMs will be provided direct to the device manufacturer responsible for integrating the SIMs into the SEMs, together with SIM data files in a standardised format containing configuration details of the SIMs provided.

This integration between the HES Vendor and the CSP shall be overseen by ESB to ensure that both parties work together to achieve the deployment timescales. ESB shall facilitate the CSP and the HES Vendors communications to ensure direct and constructive exchanges between these two parties, so that ESB's targets are achieved to meet the continued deployment of Smart Meters.

The SEM provider(s) will be responsible for integrating the suppliers eSIMs/SoftSIMs into the SEM across all meter types.

11.1.3 Coverage and performance

The communications service has the capability to establish communications and exchange commands and responses with all SEMs within the specified SLAs for device availability and

⁷ Whitelisting should be controllable via the CSP's API and via the CSP's UI.

⁸ Blacklisting should be controllable via the CSP's API and via the CSP's UI.

message round trip times, with nationwide⁹ coverage, across any of the Cellular Technologies provided.

ESB monitors KPIs and Metrics on the CSPs Network, with the Performance of the AMI solution to ensure that the de/re energisation messages are delivered to the Device Estate within the CRU SLAs. This is currently 5 mins for ESB to receive, process and transmit these messages to the SEM, with an expectation that there is around 30 seconds for the transmission over the cellular network.

11.1.4 Network improvement

The communication service supports the capability to extend the network to accommodate corresponding expansion in the ESB customer base, and to improve performance where required to meet SLAs.

11.1.5 Service reliability

The communication service incorporates component redundancy and disaster recovery systems to ensure a high degree of fault tolerance such that the failure of any single device shall not impede the communications to SEMs within SLAs. This includes the provisioning of redundant connections into ESBs IT systems at two data centres in Dublin.

11.1.6 Change of Communications Provider

The capability is available to update the SIM credentials on the SEMs remotely to allow ESB to select another Communications Provider at the end of the contract, without visiting each SEM to change a SIM card or update eSIM/softSIM credentials. In this eventuality, the HES, supported by the HES provider will interact with the CSP to manage delivery of new CSP data to the SIMs.

11.1.7 Wireless mobile telecommunications technologies

The communication service enables ESB IT systems to communicate with ESB SEMs using 4G technology. Specifically using NB IoT and/or LTE M technologies. The SEMs to be purchased by ESB will incorporate 4G (LTE M + NB IoT) communications functionality.

⁹ Nationwide should be viewed as 99.999% coverage of the population of Ireland via one or more of the cellular technologies.

12. Implementation Services

The successful Tenderer(s) will be required to provide:

- Related implementation services to install, configure and implement the proposed technical components outlined in Sections above, including specifying the infrastructure requirements and design necessary to support the effective implementation and operation of the proposed IT systems.
- Support Services for the SEM and IT Systems.
- Testing – including all test documentation, scripts, hardware, software required to conduct testing activities of all components in addition to facilitating and conducting testing of respective components and supporting ESB during the various testing phases.
- Communication – work with CSP to connect meters to the HES.

12.1 Meter+: Implementation scope for Release 1

The Implementation scope for release 1 is to support the Irish Retail Electricity Market. This is the provision of the following Single-phase SEM tariffs.

- MCC01: Single Rate Import Energy that operates 24 hours on local time.
- MCC02: two rate ToU import energy tariff that operates on UTC.
- MCC12: Import + export Power Load profile at 30min capture period on UTC time, and the A+ register that is used within the VEE processing; and
- MCC16: Ireland SST (Standard Smart Tariff) which is a three-rate import energy TOU that operates on local time.

It is expected that all four-meter configurations will operate in parallel, but it is possible that SEM limitations will cause meters to be configured to use either MCC02 or MCC16, and this may require meters to be pre-configured in the factory for either option, with configuration possible from MCC02 to MCC16 remotely.

The HES and therefore the MDMS Adaptor should be able to support the daily reading of these meter types and the ability to change the configuration to support these when CoLE or CoS occurs. There will be events recorded within the SEM that are transmitted to the HES for support of the VEE process, i.e. Time sync, Power on/off and error as a minimum so that the VEE services that support these Tariff's or MCC's can be undertaken.

It will also be necessary to support Supply Control Switch operations and P1 port operations.

These services are expected to be configuration items within the offered products and therefore, there is scope for a short design/configuration period, leading to the build and test. The HES Vendor shall ensure that their MDMS adaptor can support these minimum features and work with both Siemens and the CSP to ensure that SEMs support the full scope and are ready for installation. There shall be a capability for the HES to accept new FW and manage any campaign for the delivery of this FW to the Meter+ SEM Estate, that shall be tested and validated for minor bug fixes.

The HES Vendor shall, therefore, be expected to be operating onsite in ESB offices for this period of design configuration for the HES Solution. This enables the quick release into the build of the new environments.

The HES Vendor and the CSP are expected to work with ESB ITD to design the IT environments and APN access to support the release 1 and meter deployment.

It is envisaged that Release 1 will be a 10-month delivery which will include design, build and test and go-live during this period.

12.2 Meter+: Implementation scope for release 2

The Implementation scope for release 2 is to support the Irish Retail Electricity Market. This is the provision of three-phase whole current and three-phase and single-phase CT meters, and P1 port support for three-phase meters.

Three-Phase SEMs support MCC01, MCC02, MCC012/16 and at present do not support meter switch services. However, this may be required in future for whole current three-phase meters.

These services are expected to be configuration items within the offered products and therefore, there is scope for a short design/configuration period, leading to the build and test. The HES Vendor shall ensure that their MDMS adaptor can support these minimum features and work with both Siemens and the CSP to ensure that SEMs support the full scope are ready for installation. There shall be a capability for the HES to accept new FW and manage any campaign for the delivery of this FW to the Meter+ SEM Estate, that shall be tested and validated for minor bug fixes.

The HES Vendor shall, therefore, be expected to be operating onsite in ESB offices for this period of design configuration for the HES Solution. This enables the quick release into the build of the new environments.

The HES Vendor and the CSP are expected to work with ESB ITD to design the IT environments and APN access to support the release 2 and meter deployment.

It is envisaged that Release 2 will be a 10-month delivery which will include design, build and test and go-live during this period

12.3 HES Vendor Implementation Services

The Implementation services that ESB require of the HES Vendor have been summarised within the following section to offer a high-level understanding of the “ask”. Full and detailed requirements will be provided as part of the ITT documentation set.

12.3.1 Design of the HES System

The high-level scope of the functional and technical Design delivery of Meter+ are as follows:

- Design, configure, integrate and test the standard product offering for the HES System from the HES Vendor and associated SEMs procured from the SEM vendor(s).

- Design and delivery of all referenced business processes to allow ESB to implement, manage, support and operate the HES system.
- Integrate the HES System and associated SEMs with the selected communications service and alongside all existing HES systems.
- Design and implement the necessary infrastructure required to support the HES System, Comms service and non-production SEMs, including hardware platform, storage, switches, routers, firewalls, network configuration, middleware, operating system software, database management software, and software development tools.
- Specify, design, install, configure, integrate and test the range of different HES System environments and their associated Comms Service and SEMs. This activity is critical in enabling any application-level development, configuration and testing.
- Specify, design, build and test the physical link between ESB and the Comms Service Provider.
- The HES Vendor will also be responsible for generating or supporting the generation of the functional design deliverables that enable ESB and ESB ITS/ITD to understand and validate the design.
- Specify, design and integrate the HES Support Environment integrated into ESB processes to ensure that incidents and service requests are able to be carried out to meet ESB and ITIL compliance.

The HES Vendor is responsible for managing the key dependencies between the functional and technical design deliveries of Meter+ and ensuring that there is traceability between the ESB High level design documentation and the HES Vendors design deliverable.

12.3.2 Build of the HES System

The high-level scope of the functional and technical Build delivery of Meter+ is as follows:

- Demonstrate HES functionality for acceptance by ESB into the test and integration phases.
- Build the Development and Integration Environment, consisting of the new HES System, SEM and associated Comms service, designed in the previous phase.
- Document the detailed specification and physical design of the HES System Test Environment and Comms service. Also document the configuration and data that needs to be set on the Test SEMs and eSIMs.
- Configure the settings of the HES System, SEM and Comms service to enable the agreed scope to be tested within the development and test environments, thus allowing the testing phases to commence.
- The HES System will be deployed in ESB's data centres, which will be integrated with the Comms service via the interfaces provided within ESBs Data Centres by the Communications Service provider.
- Test SEMs will be physically located within ESB HES Technology Test Lab and will be communicating via the respective Test APN(s).
- Continue to develop the business design for how the HES System and SEM will be managed and operated by ESB.
- Preparation for the testing phases has been completed, including creation and approval of the test plan, scenarios, scripts and data. The necessary training of ESB testers will also been conducted.
- Demonstrate and integrate the HES support environment meets all requirements and support SLAs aligned with ITIL.
- Demonstrate that the required mandatory reports from the service and support environments are complete and accurate.

The HES Vendor is responsible for managing the key dependencies between the functional and technical build deliveries of Meter+ and ensuring that there is traceability between the ESB High level design documentation and the HES Vendor(s) design deliverable.

12.3.3 Test of the HES System

The high-level scope of the functional and technical test delivery of Meter + is as follows:

- Conduct a series of test phases that look to achieve, at a minimum, the following obligations through a range of checkpoints.
 - The functionality of each individual component within the HES solution for the agreed feature set has been accepted by ESB
 - The integrated components work together to provide an end-to-end process solution that delivers the scope agreed for this Stage and have been accepted by ESB.
- The agreed Build the Test Environment, consisting of the HES System, SEM and associated Comms service, designed in the previous phase.
- Document the detailed specification and physical design of the HES System Pre-Prod and Prod Environments and the configuration and data that needs to be set on the Pre-Prod SEMs must be documented
- Build the Pre-Prod and Prod Environment, consisting of the HES System, SEM and associated Comms service.
- Support the transition of the Production Environment into live operations

The HES Vendor is responsible for managing the key dependencies between the functional and technical test deliveries of Meter+ and ensuring that there is traceability between the ESB High level design documentation and the HES Vendors design and build deliverables.

12.3.4 SEM Delivery

ESB Networks will, in addition to normal industry practice, expect the vendor to be able to deliver all the devices that could reasonably be needed to conclude testing of all aspects of the HHT and consumer in-home data provision, including In-home displays, etc.

12.4 CSP Implementation Services

In general, the CSP is implemented, noting that it is likely that dedicated APNs will be needed to deliver Meter+.

13. Enduring Support Services:

The successful Tenderers will play a key role in supporting the ongoing operation of the implemented solution for the duration of the contract. A high-level description of some of the key enduring services is outlined below, however, these may be subject to change.

- Support to ESB to maintain meter services across all the deployed devices and supporting infrastructure in alignment with the contract
- Design and integration services to support current and additional Meter Vendor(s)
- Other/additional Communications Technologies in the future.
- SEM and HES System Support Services aligned with the relevant contract and ITIL
- Integration support services for third party solutions with HES.
- Testing and process support services
- Non-functional requirement validation services.
- SEM Firmware Development and supply for SEMs.

13.1 Common ITIL Services

There are a number of common Enduring services that ESB expects to be part of the ITIL solution offering for the HES and SEM Vendor(s). These are summarised within the following section. However, as the CSP is a service and the HES and SEM Vendor(s) shall provide products there are differences required by each party. These differences have been split on to the HES and SEM Vendor Sections below.

13.1.1 Incident management

An incident management system shall be deployed to support management of service requests and incidents reported by ESB. The handling of incidents shall be prioritised and in line with SLA's and shall support escalation of incidents that are business critical, recurring incidents and incident resolutions that are not being progressed.

13.1.2 Service Request management

A Service Management system will be used to manage and implement any user generated service requests from inception through to completion.

13.1.3 Problem management

The ESB definition of a problem is a set of incidents that have the same root cause and can therefore be classed as a problem. The incident management system shall also be able to deal with problem management.

13.1.4 Change management

All changes that may occur during the life of the system shall be under the remit and control of ESB. Should there be a requirement during the Meter+ lifecycle (design, build, test or hyper care) then the CSP, HES and SEM Vendor(s) will be requested to undertake Impact assessments to understand and scope the change, as part of the contract.

Should this change be requested post this period then again ESB shall manage this change and where require seek IA's from both parties to understand the scope and size of the change.

13.1.5 Contract and Service Review

It is expected that both the HES and SEM Vendor(s) will undertake regular reviews of the contract and service post hyper care periods. This is to ensure ESB, and the Vendor(s) are able to effectively manage these contracts and services and will be carried out with reference to the SLAs

13.2 HES and SEM Vendor Enduring Support Services

The HES and SEM Vendor(s) enduring support services are summarised below with additional detail to be provided within the ITT.

There are three key areas that ESB require the HES and SEM Vendor(s) to consider as part of their solution offering. These are detailed below. The HES and SEM Vendor(s) shall consider these are features of their offering and ensure that these are detailed within the ITT responses, as costed options that can be quantified and costed and correctly sized so that the experience, professional standing and costs can be compared.

13.2.1 Support for Development of New Meter Firmware

ESB understands that the essence of the HES and SEM Vendor(s) SEM offering is based on their standard FW, and through the normal Product Management of this product that other clients and the HES and SEM Vendor(s) may update the SEM FW. ESB requires that the HES and SEM Vendor(s) ensure that all FW updates are shared with ESB as part of their SEM solution offering, and that ESB has the right to reject a FW for the SEM without the SEM FW that ESB is currently using becoming end of life or incurring additional support cost from the HES and SEM Vendor(s) for the support of this FW. ESB also requires the ability to request changes to the HES and SEM Vendor(s) SEM FW throughout the lifecycle to ensure that the HES and SEM Vendor(s) SEM FW functions are fit for use based on the requirements of the ESB High level design, that will be shared with the HES and SEM Vendor(s) as part of the ITT.

13.2.2 Support for Development of New HES Features

ESB understands that the essence of the HES and SEM Vendor(s) solution offering is based on their standard product offerings, and through the normal Product Management of these products that the client and the HES/SEM Vendor(s) may update these products. ESB requires that the HES and SEM Vendor(s) ensure that all product updates are shared with ESB as part of their solution offering, and that ESB has the right to reject an update to any or all of the provided products without the product becoming end-of-life or incurring additional support costs. ESB also requires the ability to request changes to the HES and SEM Vendor(s) products throughout the lifecycle to ensure that the HES and SEM Vendor(s) solution is fit for use based on the requirements of the ESB High level design, that will be shared with the HES and SEM Vendor as part of the ITT.

13.2.3 Support for Development of New MDP/Companion Features

One of the development activities of the overall solution offered by the HES and SEM Vendor(s) is that of the creation or adoption of an Ireland or Industry Device Interoperable Standard, as such this

should be created or updated to support the requirements of ESB. Throughout the life of the HES and SEM Vendor(s) solution (i.e. minimum 15 Year) there may be an occasion for the features to be updated. The HES and SEM Vendor(s) shall be able to understand and influence the roadmap of the ROI or Industry Device Interoperable Standard to:

- Ensure that ESB understands and is updated of the developments of any of the underlying technologies or standards that the ROI or Industry Device Interoperable Standard rely upon.
- Ensure that the requirements of ESB are adopted by the ROI or Industry Device Interoperable Standard.
- Ensure that as the ROI or Industry Device Interoperable Standard evolves that ESB is updated and briefed on these developments and the impact of the AMI Solution.

13.3 Testing Services

The HES and SEM Vendor(s) are required to support AMI system testing through the lifecycle, and this will include the following services:

13.3.1 Support for test environments

Provision of a test environment for testing communications separated from the production environment.

13.3.2 Integration and testing resources

Provision of resources to support installation, commissioning and testing activities, within the hyper care period and with the onboarding of new devices into the AMI system. In addition, performance testing of the HES and associated AMI interfaces may utilise appropriate simulation and performance testing tools, including independent meter test tools or vendor-provided performance test tooling, to validate high-volume transactions and key SEM-HES exchanges.

13.3.3 End device approval testing

Provision of an approval service to assure that any communications interface embedded into a SEM developed for this system is compliant with the minimum specification of the communications interface as specified in Implementation Services: Design of the communication service above and can be integrated into the communications network.

Ensure that previously assured modems continue to operate correctly for the life of the SEM on the communications network.

13.3.4 Cyber Security Testing

ESB undertakes a range of cyber security testing activities, including Meter Teardown Testing, cyber-simulation exercises, and various levels of IT/OT penetration testing across all systems. In addition, increased vigilance from regulatory bodies requires a continuous cyber-assurance approach to demonstrate alignment with regulatory expectations.

Vendor(s) are required to support these testing activities and as contractually bound, provide ESB with the necessary assurances regarding their cyber-security controls to satisfy external regulatory

bodies (e.g., annual ISO27001 certification). Vendor(s) are also expected to participate in the cyber-assurance activities identified by ESB and its approved advisors to facilitate compliance prior to any formal regulatory assessment. As part of these processes, Vendor(s) work with ESB on risk assessments and carry out agreed remediation activities for identified risks. This includes a clear commitment to remediate any deficiencies highlighted through the testing and assessment activities, ensuring that issues identified during assessment are addressed in an effective and timely manner.

13.3.5 SEM Delivery

The SEM Vendor(s) shall have the capability to notify ESB of the shipment status of SEM orders and associated status that may affect the delivery or replacement of SEM.

13.3.6 Firmware issues

The HES and SEM Vendor(s) shall have the capability to ensure that the currently in operation FW or SW that the HES or SEM is operating with is supported and updated for the duration of the life of the application or device.

13.3.7 SEM, HES and Security Incidents

The HES and SEM Vendor(s) shall have the capability to monitor and report on current and historical incidents, problems and changes that have been applied to the SEM and or HES throughout the lifecycle and for a duration of 15 years to support the operational life of the system and SEM.

The SEM Vendor shall have the capability to analyse all faulty SEMs returned to them by ESB for examination and shall report all findings to ESB accordingly.

The HES and SEM Vendor(s) shall have the capability to monitor and report on security incidents, such as defects within their products security design, and ensure that ESB is apprised of these and any mitigation actions that should be undertaken.

13.3.8 Troubleshooting

The HES and SEM Vendor(s) shall provide tools to enable business users to troubleshoot HES and SEM issues, along with providing support for the identification of trends and problems.

13.3.9 Documentation

Service Management process documentation will include at least the following for review and agreement by ESB:

- Logging and tracking of Service Requests from the ESB made via the vendors Service Desk.
- Categorising and prioritising Service Requests according to agreed criteria.
- Following appropriate approval procedures (including as specified by the ESB).
- Sourcing and delivering Service Requests.
- Notifying ESB following completion (and reopening if necessary) via agreed Service Desk processes.
- Providing information to ESB Service Desk about services and procedures for obtaining them.
- Assisting ESB Service Desk with general information, complaints and comments.

- A full software bill of materials showing the versions of all software and any specific hardware required to create, build and deploy the HES and KMS applications.

13.4 CSP Enduring Support Services

These are already in place.

14. Glossary

Table 7 – Glossary

Term	Description
Access Point Name (APN)	The name of a gateway between a GSM, GPRS (2G), 3G or 4G mobile network and another computer network.
AC Electricity Smart Meter Generic Companion Profile (ACE SM GCP)	A DLMS/COSEM-based companion specification defining the standardised data model and interoperability framework for smart electricity meters.
Advanced Encryption Standard	Specification for the encryption of electronic data approved for use by the US government and accepted worldwide.
Advanced Metering Infrastructure (AMI)	The full measurement and collection system including smart meters, communications networks and central AMI systems for data management and operational use.
Alert (Metering)	A message from the SEM to the CCS providing immediate notification of a configured Event.
Application Programming Interface (API)	A defined interface of code and specifications enabling software programs to communicate with each other.
Asymmetric Keys	Security credentials using different keys for protecting and validating/decrypting information.
Authorised User	A user or entity granted access to a system or resource.
Auxiliary Load Control Switch	A SEM switch configurable to control night storage heating or other loads.
Auxiliary Switch Connection	SEM terminals used to apply the Auxiliary Load Control Switch.
Bi-Monthly	Occurring every two months.
Black Box Testing	Testing methodology without knowledge of internal implementation (SP 800-53A).
Blacklist	SEMs/SGDs not authorised to communicate with the HES.
Blacklisting	Removing a SEM from the whitelist and adding it to the blacklist.
Bulk Operation	Processing a large block of data in a single transaction.

Business Continuity Plan	Defines steps to restore business processes after disruption; includes triggers, roles, communications.
Business Service Request (BSR)	Request to carry out an action or read information on a Smart Device.
Certificate Authority	Entity issuing digital certificates upon validation of a Certificate Signing Request.
Certificate Signing Request (CSR)	Message sent to a Certificate Authority to request a digital certificate, typically containing a public key.
Change Advisory Board (CAB)	Body that approves changes, assesses impacts and liaises between parties.
Change Management Governance Forum	ESB–CDSP joint group reviewing BAU change and approving major changes.
Change Request (Project)	Documented request to change the project’s functional or non-functional requirements.
Collected Data Packages	Daily messages containing consumption and event data collected from Smart Devices.
Connect / Disconnect	Whether the internal Supply Control Switch is open or closed
Command	Instruction created within the AMI system for execution on a Smart Device.
Command Response	Message from a SEM in response to a Command.
Commission for Regulation of Utilities (CRU)	Regulatory authority for the Irish energy sector, including NSMP governance.
Comms Module Specification	Specification defining performance and functional requirements of the Electricity Comms Module.
Communication Network	All wired/wireless networks, software and infrastructure used to convey data between SEMs and ESB systems.
Communications Function	SEM or companion device providing WAN connectivity and optional IHC connectivity.
Communications Service Provider (CSP)	Provider offering cellular communications services for AMI.
Communications Service	The cellular connectivity enabling data exchange between SEMs and ESB systems.

Connection Establishment	The process of establishing IP communications between a SEM and the HES (e.g., PDP context for 2G).
Consumer Access Device	A consumer device attached to the IHC for energy monitoring/control.
Core Network	Mobile core network components (e.g., GGSN, SGSN, M2M platform).
CTF – Communications Technically Feasible	ESB methodology to determine whether a device can perform Smart Services reliably.
Cyber Security	Techniques to protect systems and data from unauthorised access or attacks.
Cyber Resilience Act (CRA)	Proposed EU regulation establishing cybersecurity standards and ongoing security obligations for digital and IoT products, including smart meters and supporting systems.
Data Centre	Facility housing computing, storage and telecommunications systems.
Data Collection	The process of collecting data from SEMs by the AMI solution.
Data Collection Packages	Nightly payloads including encrypted registers, logs and event data.
De-Energise	Disabling customer supply by opening the SEM switch (remotely or locally).
Design Level Review	Security review of a product's design and documentation.
Digital Signature	Electronic signature proving message authenticity and integrity.
DLMS/COSEM	Internationally adopted smart metering protocol suite used as the AMI Meter Data Protocol (MDP). Governs object models, secure messaging, data profiles and interoperability.
Distribution Asset Owner Licence	Licence under the Electricity Regulation Act permitting distribution asset ownership.
Distribution System Operator Licence	Licence under the Electricity Regulation Act permitting distribution system operation.
Dual Authorisation	Requirement for multi-party approval when issuing critical commands through AMI or ESB systems.
Electricity Meter	Device measuring and recording electricity consumption.
Electricity Supplier	Licensed entity supplying electricity to consumers.
Electricity Supply Board	Statutory corporation headquartered at Fitzwilliam Street, Dublin.

Encrypt	Protecting data by applying an algorithm to obscure plaintext.
ESB 18080	ESB specification covering general materials, equipment and works.
ESB Networks	Combined ESB group networks organisations (TAO/DAO and DSO activities).
ESB Networks DAC	Registered company operating the DSO functions.
Event and Alert Management Strategy	Defines which activities raise events/alerts and how they are collected or transmitted.
Exception	Unexpected error/event preventing normal process completion.
Export Register	Record of exported energy (kWh).
Firmware Management Agreement	Agreement between ESB, meter Vendor(s) and tenderer governing firmware development/testing.
Fragmentation	Splitting a payload into segments when exceeding MTU size.
Good Manufacturing Practice	Certified standard for manufacturing quality and control (e.g., ISO 9001).
Hardware Security Module (HSM)	Secure ESB-hosted component for key generation, storage and cryptographic operations (FIPS 140-2 L3).
HHT (Hand-Held Terminal) – LMOT (Local Meter Operations Terminal)	Field technician portable device used to interface locally with SEMs. Known internally in ESB as LMOT; “HHT” used in this document for external clarity.
Hypercare	Period following cutover where enhanced support is provided.
Identity and Access Management	Processes ensuring correct privileges and identities access resources appropriately.
IHC Device List	List of permitted devices for an IHC Network Control.
IHC Network Control	Element within the In-Home Channel managing connected devices.
Import Register	Record of imported energy (kWh).
Incident	Unplanned interruption or degradation of an IT service.
In-Home Channel	Mechanism conveying consumption data to devices in customers’ homes.

In-Home Channel Dataset	Data items available for IHC-connected devices.
In-Home Channel Host	Hardware/software providing Home Area Network functionality.
In-Home Data	Predefined consumption data shared into customer premises via secure channel.
In-Home Device	Device using IHC data (e.g., In-Home Display, home gateway).
Inter Participant Test	Testing NET ISU market processes with suppliers and verifying interoperability.
Internet Protocol Link	Links between ESB and CSP data centres enabling system-to-system communication.
Interval Data Profiler	SEM store capturing interval consumption data.
Intrusion Detection System (IDS)	System monitoring for suspicious or malicious activity.
Intrusion Prevention System (IPS)	IDS that actively blocks malicious activity.
Knowledge Management	Processes/systems for storing and sharing knowledge and information.
kVAr / kvar	Unit representing reactive energy.
Lead Consortium Member	Nominated lead entity within an applicant consortium.
Legacy Electricity Meter	Older electro-mechanical/electronic electricity meter replaced by smart meters.
Load Limiters	SEM function disconnecting supply when consumption exceeds thresholds.
Local Interface	SEM interface used by field technicians to access meter data/commands.
Local Network	In-premises network connecting utility devices and other devices.
Local Network Access Point	Device controlling access to a local network.
Long Term Evolution for Machines (LTE-M)	A low-power wide-area cellular technology suitable for IoT/metering applications requiring higher bandwidth and mobility than NB-IoT.
Machine-to-Machine (M2M)	Machine communication over wired/wireless channels.

Major Incident	Incident with significant business impact.
Maximum Demand Registers	SEM registers storing maximum averaged load values.
Meter Configuration Code (MCC)	Code defining Smart Data Service levels for suppliers.
MCC01	24-hour import energy register service.
MCC12	30-minute import interval service.
MCC16	Day/Peak/Night ToU register service under CRU tariff.
Meter Data Protocol (MDP)	Protocol rules used by AMI systems to communicate with SEMs. For this programme, MDP = DLMS/COSEM.
Meter Vendor(s)	Entities supplying SEMs.
Meter/Module Integration Specification	Specification defining integration of Comms Modules with SEMs.
Measuring Instruments Directive (MID)	EU directive defining requirements for accuracy, conformity assessment, and performance standards for measuring instruments such as electricity meters.
Micro-generation	Micro-generator use up to 6 kVA (1-phase) or 11 kVA (3-phase).
Mounting (a Smart Meter)	Physical installation of a SEM at a premises.
Meter Data Management System (MDMS)	A centralised IT system that receives, validates, stores, and processes smart meter data (e.g., interval data, events, alerts), and provides data to enterprise systems such as billing, customer service, and analytics.
Meter Point Registration Number (MPRN)	Unique identifier for a location supplied with electricity.
Narrowband Internet of Things (NB-IoT)	A low-power wide-area (LPWA) cellular communications technology used for reliable, long-range, low-bandwidth metering communication.
Near Real Time	Data made available with minimal delay, limited to communication/processing time.
Network Design	Design of systems/architecture for enduring communication services.
Network Operations Centre (NOC)	Centralised function controlling and monitoring services.

Operational Support Systems (OSS)	Software for managing infrastructure, networks, and systems.
Optical Port	Infrared SEM port for data transfer.
Packet Data Protocol (PDP)	Protocol enabling packet network communication with GPRS.
PDP Context Activation	Process establishing connectivity on GPRS networks.
Performance	Consistent, efficient achievement of service outcomes.
PKCS#11	Open standard defining cryptographic token interfaces.
Power Quality Profiler	SEM store capturing electrical quality parameters.
Powering Up (a Smart Meter)	Activating a mounted SEM by installing the main fuse.
Pre-Qualification Questionnaire (PQQ)	Document issued to shortlist applicants.
Private/Public Keys	Cryptographic key pair enabling encryption and signature validation.
Protocol Companion Specification	Specification defining how protocol features are applied for commands, responses and alerts.
Protocol Technical Authority	Body maintaining protocol (e.g., DLMS UA, ZigBee Alliance).
Provisioned	Communications Module that has completed all post-registration processes.
Public Key Infrastructure (PKI)	Framework for managing digital certificates and key pairs.
Quality	Degree to which a service/process provides intended value.
Radio Chipset	IC components forming a radio transceiver.
Reactive Consumption Measurement	Measurement of wattless energy.
Reassembly	Rebuilding fragmented payload data.
Re-Energise	Restoring supply by closing the SEM switch.

Role-Based Access Control (RBAC)	Restricting access based on defined user roles.
Roll Back	Reverting to a previous firmware version.
Security Incident and Event Management (SIEM)	Tools/processes providing centralised correlation of security logs/events.
SEM Event Identifier	Number representing a specific SEM event type.
SEM Event Log	SEM log storing event information.
Service Asset Configuration Management	Controlling assets/configuration data required for service delivery.
Service Desk	Single point of contact for users; manages incidents and service requests.
Service Level	Measurement of performance against service targets.
Service Switch	SEM switch capable of de-energising/re-energising supply.
Short Outage	Outage lasting less than 3 minutes.
Smart Device	A SEM or separate Communications Function device.
Smart Electricity Meter (SEM)	Smart meter with remote communication, switching and data capture functions.
Smart Meter Deployment	Replacement of legacy meters with SEMs.
Smart Metering Ecosystem	SEM, WAN and associated AMI systems/services using the MDP.
Software Bill of Materials (SBOM)	A formal record containing the details and supply chain relationships of software components used within a system or device, supporting security, compliance, and vulnerability management.
Standardised Smart Tariff	Tariff where switching times are set by CRU.
Subscriber Identity Module (SIM/eSIM)	Secure component storing mobile subscriber identity and keys.
Supply Control Switch	SEM switch enabling or disabling customer supply.
Timestamp	Recorded date/time of an event or log.

Transmission Asset Owner Licence	Licence under the Electricity Regulation Act permitting transmission asset ownership.
Validation, Estimation and Editing (VEE)	Processing to validate, estimate and correct metering data.
Virtual Private Network (VPN)	Secure encrypted communication channel over insecure networks.
Wake-Up	Signal instructing a SEM to begin connection establishment with the HES.
Watt-hours (Wh)	Unit of energy (1 Wh = 3600 J).
Watts	Unit of power.
White Box Testing	Testing using full knowledge of internal structure (SP 800-53A).
Whitelist	SEMs/SGDs approved to communicate with the HES.
Whitelisting	Adding a device to the Whitelist.

15. Capability Descriptions (Selected)

Table 8 – Selected Capability Descriptions

ID	Capability Title	Capability Description
5.4.1	AMI Operations Strategy & Planning	Defines how ESB Networks will operate the AMI solution over time, including objectives, roadmaps, and governance. Sets priorities for features, upgrades, and operational improvements to ensure reliability, regulatory alignment, and value for money.
5.4.2	AMI Data & Message Management	Governs how meter/device messages and AMI data are structured, exchanged, validated, and stored across the HES, MDMS and related systems. Ensures consistent formats, integrity, and traceability so operational and market processes run reliably.
5.4.3	Manage Meter Data Retrieval	Plans and executes scheduled and ad-hoc remote reads (interval and non-interval) from smart meters. Ensures timely, accurate retrieval to support billing, settlement, operations, and exception handling.
5.4.5	Communications Service Management	Manages the services provided by communications provider(s) for the AMI wide-area network. Covers service classification, capacity and performance monitoring, incident management, and optimisation of message flows and costs.
5.4.6	AMI Service Management	Runs day-to-day AMI operations across incidents, problems, and changes, including vendor interactions and post-go-live support (e.g., warranty/hyper care). Maintains service levels and coordinates fixes across the AMI ecosystem.
5.7.1	Meter Asset Strategy & Specification	Sets the overall meter asset strategy and defines the smart electricity meter (SEM) specifications and compliance standards. Governs how specifications evolve to meet regulatory and operational needs.
5.7.2	Meter Asset Registration	Controls the onboarding of meter assets and their attributes into core systems (e.g., SAP, MDMS, HES). Ensures accurate identification, status, and distribution of asset data to downstream stakeholders and services.
5.7.3	Meter Asset Replacement Management	Plans and executes targeted or mass meter replacements (e.g., end-of-life, performance issues). Tracks progress, status updates, and post-replacement validations to maintain asset integrity.
5.7.4	Meter Asset Testing	Assures meter quality through acceptance testing, ongoing batch QA, and issue investigation. Includes management of test environments and evidence to support decisions and warranties.
5.7.5	Meter Asset Performance Management	Monitors meter field performance, consolidates failures/faults, and analyses trends to drive corrective actions and recalls where needed. Manages related warranty claims and supplier follow-ups.

5.7.6	Meter Firmware Management	Plans, tests, approves, and deploys firmware updates to the meter estate in a controlled manner. Confirms secure distribution, successful activation, and estate-wide version compliance.
5.7.7	Device Configuration Management	Defines and governs device technical and market configurations, including release, deployment campaigns, and audit trail. Ensures changes are tested, approved, and traceable through AMI systems.
5.7.8	Device Event & Alert Management	Sets the strategy and rules for generating, filtering, routing, and reporting device events and alerts. Enables timely triage and action by operational teams and downstream systems.
1.9.1	Security Oversight and Cyber Risk Management	Establishes governance, risk appetite, and the method to identify, assess, and treat cyber risks across the smart metering landscape. Provides ongoing visibility and assurance to stakeholders through structured oversight.
1.9.2	Data Privacy and Protection	Applies data classification and protection controls to safeguard personal and sensitive information throughout AMI processes and integrations. Ensures compliance with applicable privacy and data-protection regulations.
1.9.3	Identity and Access Management	Manages user and system identities and their privileges across AMI IT/OT components. Enforces least-privilege, segregation of duties, and periodic recertification to reduce unauthorised access risk.
1.9.4	Security Operations, Vulnerability Management and Incident Response	Monitors, detects, and responds to cyber threats affecting AMI systems; manages vulnerabilities through assessment and remediation. Coordinates incident containment, recovery, and lessons learned to strengthen overall resilience.