PAS 1878:2021, Energy smart appliances – Classification – Specification

There are several instances of red boxed text in the draft. These do not form part of the draft itself; rather, they are notes to the reader to invite comments on particular subtopics within the draft.

Contents

List of figures

List of tables

Foreword

Publishing information

This PAS was sponsored by the Department of Business, Energy and Industrial Strategy (BEIS) and the Office for Low Emission Vehicles (OLEV). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on [DD MM YY].

Acknowledgement is given to the technical author, and the organizations that were involved in the development of this PAS as members of the steering group:

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a specification to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Relationship with other publications

This PAS is developed in parallel with PAS 1879: *Energy smart appliances – Demand side response operation – Code of Practice*.

Information about this document

Assessed capability. Users of this PAS are advised to consider the desirability of quality system assessment and registration against the appropriate standard in the BS EN ISO 9000 series by an accredited third-party certification body.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at bsigroup.com/standards, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Use of this document

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The provisions of this PAS are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is “shall”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Requirements in this PAS are drafted in accordance with *Rules for the structure and drafting of UK standards:2017*, subclause **G.1.1**, which states, “Requirements should be expressed using wording such as: ‘When tested as described in Annex A, the product shall ...’”. This means that only those products that are capable of passing the specified test will be deemed to conform to this PAS.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction

0.1 Purpose

The purpose of this PAS is to enable standardized control of energy smart appliances on an electricity network in order to:

- match the short-term availability of intermittent generation sources such as wind and solar renewable energy;
- decrease the peak load on transmission and distribution networks and so to alleviate the need for network upgrades to handle new domestic appliance types, such as electric vehicle (EV) chargepoints and electric heating, ventilation and air-conditioning (HVAC) systems;
- allow control of electricity network characteristics such as line frequency, system inertia, network voltage and provide immunity from network and generation outages; and
- allow electricity suppliers to offset their short-term market imbalance by controlling flexible load on the network.

These aims are achieved by shifting (in time) and/or modulating (increasing or decreasing) the collective electricity consumption or production of domestic appliances, in line with consumer preferences and agreement, in response to signals from grid-side actors (including but not limited to aggregators, virtual lead parties, asset operators, etc.).

At longer timescales and with sufficient notice, this can be achieved through electricity suppliers, by altering the tariff that electricity consumers pay, to encourage the use of appliances at times outside of peak demand or at times when excess or renewable generation capacity is expected to be available. This is called the ”tariff-based” method. Electricity suppliers might set time of use (ToU) tariffs on either a static, repeating, or dynamic basis. In the dynamic case, the tariffs are typically set at a minimum periodicity of one day and at an increment of no less than 30 min. At shorter timescales, for rapid load responses and for control by other grid-side actors, direct control of load is required, and consumers are rewarded for allowing their appliances to be controlled for the overall benefit to the network. This is called the “called” method. These methods are collectively called demand side response (DSR).

These methods aim to provide benefits to all electricity consumers. Such benefits might be indirect, as domestic appliances providing DSR services support network operation, which benefits all consumers connected to the network. These benefits might also be direct, as consumers with ESAs can reduce their electricity costs by operating domestic appliances on ToU tariffs, and can earn revenues by allowing domestic appliances to be controlled flexibly. Actors providing these revenue opportunities to consumers are encouraged to make these benefits clear, to encourage the uptake of domestic appliances able to support network operation. It is also expected that other energy-related services might be offered in addition to the minimum specification set out in this PAS. These include other services, such as optimization of rooftop solar self-consumption with appliances or battery storage, that can provide additional benefits for consumers.

This PAS provides a technical specification that allows domestic appliances to operate in such a DSR system.

0.2 Demand side response and energy smart appliances

DSR requires communication between domestic appliances and a controlling entity, which itself communicates with the appropriate transmission system operators, distribution system operators and optionally electricity meter controlling organizations. This controlling entity is termed the “DSR service provider” (DSRSP) in this PAS. More than one DSRSP might be associated with a single premises at any one time but an appliance is associated with only one DSRSP at any one time.

The role of the DSRSP and the environment in which it operates will be described in PAS 1879, due for publication in 2021.

To provide DSR services, a domestic appliance needs to shift in time and/or modulate in magnitude its electricity consumption or production, in response to external signals. Domestic and light commercial electrical appliances are termed “energy smart appliances” (ESA) when they:

a) use a dedicated energy smart communications interface to:

   1) provide status and forecast information concerning their energy use to other devices; and

   2) receive energy-related information and instructions from other devices; and

b) meet the other requirements specified in this PAS.

In this PAS, the ESA is required to provide information for options on how it is able to modulate its power requirements over time – its power “flexibility” – over this communications interface.

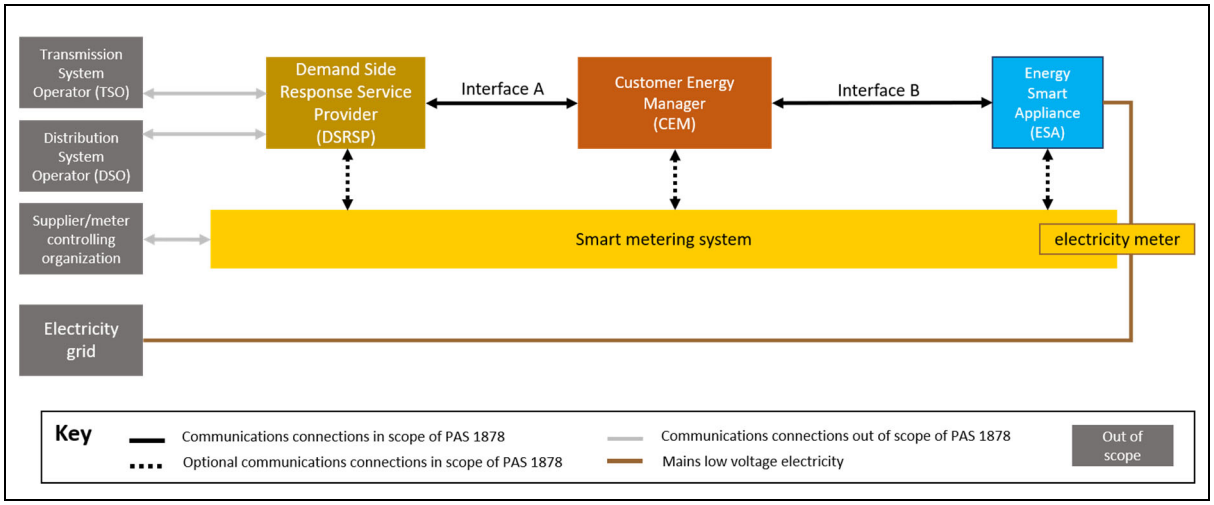
ESAs currently covered in this PAS include domestic smart EV chargepoints, electrically powered heating, ventilation and air conditioning (HVAC), battery storage, wet appliances and cold appliances, but the ESA classification is not limited to these appliances; if an appliance not listed meets this specification it can be considered an ESA. The technical requirements an ESA will need to meet in order to provide DSR services are specified in this PAS and a summary is shown in Annex E.

In order to be able to control demand and supply on electricity transmission and distribution networks for the purposes shown in **0.1**, a number of DSR products need to be procured by electricity network stakeholders, examples are shown in Annex C. These include both products that are grid frequency sensitive (e.g. frequency response products) and those that adjust demand or supply to affect the power balance (e.g. turn up or turn down reserve products) and requiring different response times. DSR might be required in different geographical areas and at different times of day in order to operate the system where or when there are network constraints. The minimum volume thresholds of services needed to have an effect require many domestic ESAs to be aggregated together on a statistical basis. A description of typical requirements for DSR products by grid-side actors is shown in Annex C.

This PAS provides a minimum specification for functionality, information flow, communications capability and cyber security for the DSR-only aspects of an ESA. This minimum specification gives a sufficient level of interoperability, security and optionality whilst not limiting the opportunity for product and service innovation.

Functionality in addition to that offered by these ESAs, such as communications gateway functionality [depicted as “customer energy manager (CEM)” and “ESA gateway (ESAG)” in Figure 1], is also required in an end-to-end DSR system and is treated in this PAS as a necessary component of the entire system.

Figure 1 – Logical DSR architecture and communications connections described by PAS 1878



In order to support a minimum level of DSRSP and ESA interoperability for every ESA type, this PAS requires that each ESA is supplied with a CEM and an ESAG. These are logical entities and can be provided with the ESA in a number of ways. For example, they can be built into the ESA, supplied as separate physical units, provided as software operating in the cloud or another device such as a mobile broadband station, or provided as part of the smart metering system. One CEM could connect to multiple ESAs. A combined CEM/ESAG can be offered. In this PAS, “CEM” also indicates a CEM/ESAG combination or an individual CEM as appropriate unless otherwise stated.

0.3 Operational model

The DSR system operates in the following manner, in accordance with Figure 1 and as illustrated in Figure 2 (where the CEM and ESAG have been combined for the sake of clarity).

a) The ESA determines its flexibility options (taking into account customer preferences and optionally electricity tariffs) and provides them to the DSRSP, using the CEM/ESAG as an intermediary. The CEM communicates with the DSRSP using a common interface specified in this PAS.

b) This information is updated whenever the flexibility status of the ESA changes (e.g. the consumer turns the ESA on or off) or a flexibility option is no longer valid (e.g. it has expired or been cancelled by the consumer).

c) The DSRSP maintains an up-to-date list of the possible flexibility options for each ESA.

d) Whenever the DSRSP is requested to perform a DSR operation, the DSRSP is able to choose from its list of ESAs and flexibility options.

e) The DSRSP then sends a message to a selected number of ESAs, via their CEMs, requesting that they implement one of their provided flexibility options. The ESA implements this flexibility option and enters response mode.

f) During the DSR event period:

   1) each ESA continues to provide the DSRSP with updated flexibility options whenever its flexibility status changes. The DSRSP may respond by sending an updated flexibility option request;

   2) if the DSRSP decides to cancel the participation of a particular ESA in the current DSR event or if the DSR event is cancelled, then the DSRSP informs the ESA, via

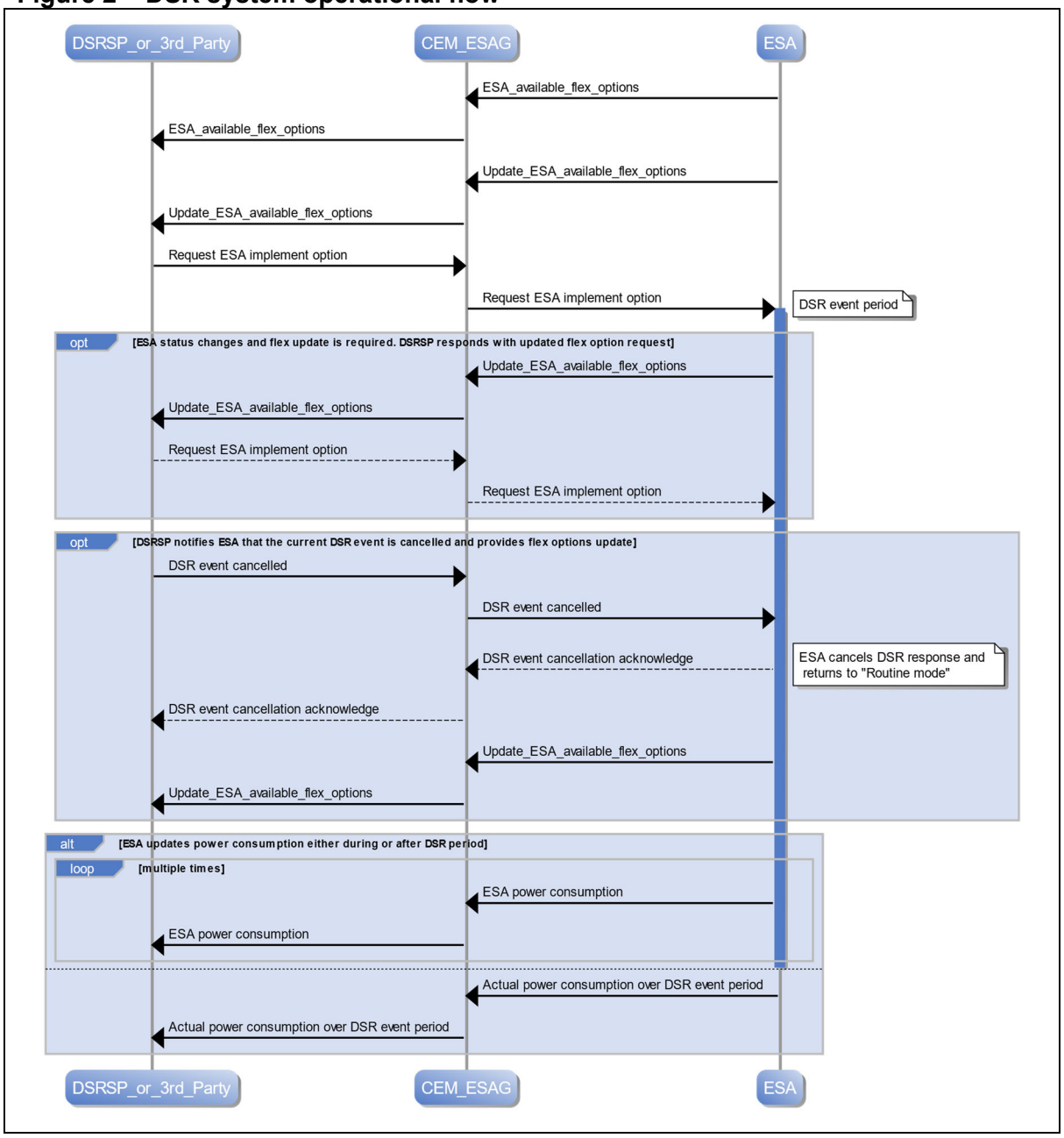
the CEM. The ESA acknowledges this cancellation, enters routine mode and sends an updated set of flexibility options to the DSRSP;

3) depending upon the requirements of the DSRSP and subject to prior agreement, the ESA might periodically send power consumption information to the DSRSP

g) Once the DSR event period is completed, the ESA provides the DSRSP with information concerning its power consumption throughout the period. This step might be omitted if the ESA has been providing periodic power consumption information.

h) The DSRSP is then able to provide aggregated flexibility verification information to the grid-side actor which requested the DSR service (including real-time power consumption values).

Figure 2 – DSR system operational flow



0.4 Alignment with DSR and ESA policy principles

There are four policy principles that are seen as critical for effective DSR through ESAs. This PAS aligns with these principles as described below.

a) **Interoperability:** The ability of an ESA to work seamlessly across any appropriate DSR service operated by any authorized system actor. In order that DSR signals can be communicated to all ESAs, open standards to support interoperable commands and languages are essential for enabling free consumer choice, and thereby a competitive market. Communications to and from the ESA to the DSRSP are necessary.

   The key aspect of interoperability in this PAS is to allow a consumer to switch an ESA to a different DSRSP at any time and maintain DSR functionality without the need to purchase or install any new equipment, or the need for a home visit from an installer or supplier of equipment. This is supported by the definition of the minimum required common data model, information model and communication protocol, performance and security requirements for the interface between the DSRSP and CEM.

b) **Data privacy:** The secure transmission and storing of data on the device or with any controlling party. Only the minimum amount of data needed to operate a DSR service is shared with DSRSPs. Consumers need to be in control of any data exchanged with third parties arising from the ESAs, with clear consent procedures that allow them to make informed decisions regarding data sharing and to update their consent as appropriate.

   Personal data, if required, is stored in a secured area in an ESA and all communication in the DSR system includes authentication and encryption. Personal data is transferred between components of the DSR system only if absolutely necessary, and is limited as much as possible. Such data is not transferred without the knowledge and permission of the consumer. Data privacy standards and guidelines are referenced as appropriate.

c) **Grid stability:** The prevention of outages on the grid caused by inappropriate operation of ESAs. Consideration should be given to the security of electricity supply, to ensure that ESAs would not represent a risk to its stability.

   NOTE 1 The ability to shift or modulate the electricity consumption or production of ESAs, as specified in this PAS, contributes to maintaining electricity grid stability. This principle focuses on avoiding any ESA operation which could unintentionally be detrimental to grid stability e.g. large load swings at the exact time when a tariff changes price or ESAs flexibility information being out of date when called for a response.

   ESAs update their flexibility information to DSRSPs whenever their flexibility status changes, so DSRSPs have an up-to-date knowledge of the flexibility available and can iteratively call responses. CEM operation modes are defined with a control hierarchy so that consumer wishes are respected and electricity network operator needs are met.

   The DSRSP is able to determine whether or not each DSR event is subject to a randomized timing offset if it decides that such an offset is necessary for grid stability.

   In the case of exception conditions (e.g. power loss), the ESA transitions or resets to a mode that brings it into a safe state. This depends upon the ESA type and the manufacturer. The ESA reports its change in flexibility status to the DSRSP whenever possible.

   In the event of a loss of communications between the ESA and the DSRSP, the ESA continues with its currently selected flexibility option and logs its power consumption periodically for transmission to the DSRSP whenever communications are resumed. The DSRSP is able to include a timeout value in the flexibility option request message to a CEM or ESA, upon the expiry of which the ESA reverts to routine mode if it has not already done so.

d) **Cyber security:** the appropriate protection of ESAs from unauthorized access and the correct use of ESAs by authorized parties only in order to achieve valid DSR events. This includes information security of the ESA itself, messages sent between authorized

parties and the ESA, as well as the security of local (i.e. home area network) and/or cloud-based networks through which third parties can communicate with ESAs. ESAs, control systems, including those used by DSRSPs, and communications between these parties are covered by this principle. Both consumers and electricity network operators need confidence that ESAs are cyber secure for safety and privacy.

Cyber security is an important aspect of the DSR system. This PAS specifies minimum requirements for the storage and exchange of information between the DSRSP and ESA, and for the authentication of the DSRSP, the CEM, the ESAG and the ESA.

An ESA is required to meet baseline device authentication and verification, including software and firmware checks and updates, communications authentication/encryption and secure data management criteria. Cyber security standards and guidelines are referenced as appropriate.

NOTE 2 An end-to-end cyber risk analysis is included in the Annexes to PAS 1879.

0.5 Integration with smart metering systems

DSR operation of ESAs defined within this PAS does not require the use of a smart metering system, but is fully compatible with smart metering systems. The options for combining the DSR system architecture with the GB smart metering system specifically are described in Annex D. The DSR architecture does not exclude combination with other smart metering architectures.

0.6 Alignment with standards

Domestic DSR standardization is currently at an immature stage and work is ongoing within European and International level standards development organizations. The architecture presented in this PAS is aligned with this work carried out in several CEN/CENELEC and ISO/IEC Technical Committees including, IEC TC57 “Power systems management and associated information exchange”, CENELEC TC205 “Home and building electronic systems”, and CENELEC TC59X “Performance of household and similar electrical appliances”.

This PAS presents several candidate standards for use at various points in the architecture, which are likely to be refined as a consequence of ongoing work in BSI and elsewhere.

It is possible that proposals to European or International standards’ groups might be required in order to align their publications with this PAS exactly (for instance, by specifying a national profile or an extension to an information model).

1 Scope

This PAS specifies requirements and criteria that an electrical appliance needs to meet in order to perform and be classified as an energy smart appliance (ESA). It defines the attributes, the functionalities and performance criteria for an ESA, and specifies how compliance with these can be verified.

This PAS covers:

- the generic, or specific, functional requirements of ESAs, which enable the performance of DSR-based activities;
- the ESA system architecture for DSR-based activities, including communication links and object functionalities and, in particular, the interfaces between the CEM and the ESA and between the CEM and the DSRSP;
- the ESA operational sequence of DSR-based activities, including communication protocols where necessary; and
- relevant ESA lifecycle considerations.

This PAS also covers compatibility with smart meter technologies, specifically full compatibility with the GB smart metering system.

This PAS applies the following criteria in defining the requirements that are to be met by an ESA performing DSR-based activities.

- **Interoperability:** the ability of an ESA to work seamlessly across any appropriate DSR service operated by any authorized system actor.
- **Data privacy:** the secure transmission and storing of data on the device or with any controlling party.
- **Grid stability:** the prevention of outages on the grid caused by inappropriate operation of ESAs.
- **Cyber security:** the appropriate protection of ESAs from unauthorized access and the correct use of ESAs by authorized parties only in order to achieve valid DSR events.

For requirements relating to compatibility with all forms of DSR-based activity, two types of DSR are covered in detail:

- supplier/utility set electricity tariffs; and
- TSO/DSO requested services with responses called by DSRSPs (transmission and distribution network level, including grid frequency sensitive).

This PAS specifies the minimum requirements to perform these DSR-based activities, in line with the four criteria above.

This PAS covers the following electrical appliances that are used in a domestic or small business settings[1)]:

- heating, ventilation and air conditioning (HVAC) appliances;
- cold appliances;
- wet appliances;
- battery storage; and
- smart EV chargepoints.

[1)] In the UK, this PAS is most applicable to customers in Profile Class 1 – Domestic Unrestricted Customers and Profile Class 2 – Domestic Economy 7 Customers, as defined by Elexon: https://www.elexon.co.uk/operations-settlement/profiling/.

This PAS does not cover:

- the deployment and functional configuration of the wider DSR environment;
- standards implied by existing relevant overarching regulation, for example the general safety or other aspects of the non-smart functionality of an ESA; and
- contracting, payment services or general consumer protections.

This PAS is intended to be used by manufacturers of ESAs and CEMs. Other actors who might have an interest in this PAS are maintainers of ESAs, manufacturers and maintainers of interfacing products, software developers and service providers.

The specified characteristics of an ESA are complementary with the DSR environment in which it operates which will be described in PAS 1879 (due for publication in 2021), as the characteristics enable the ESA to perform DSR-based activities.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions of this PAS[1)]. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ETSI TS 303 645, *Cyber security for consumer Internet of Things*[2)]

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

3.1.1 active period
period within a power profile for which the power value is non-zero

3.1.2 appliance
product or system that consumes, stores or generates electrical energy during its functional use

3.1.3 appliance controller
sub-system of an appliance responsible for controlling the operation of the appliance machinery and power sub-system

3.1.4 appliance machinery
part of an appliance that carries out the main functions of the appliance

3.1.5 auxiliary proportional controller (APC)
device controlled by the GB electricity smart metering equipment and capable of selecting one of a range of values

3.1.6 cold and wet appliances
electrical goods used in a domestic or small business environment, for example refrigerators, tumble dryers and washing machines

3.1.7 consumer
domestic (i.e. individual households) or small business user (i.e. small and medium-size enterprise) who:

[1)] Documents that are referred to solely in an informative manner are listed in the Bibliography.

[2)] Available at https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.

a) has the authority to enter into a service contract with a DSRSP; and

b) has one or more ESAs that can be subscribed to a DSR service

3.1.8 consumer access device (CAD)
physical or logical device that links the GB smart meter HAN and the consumer HAN, which is permitted to extract real-time energy and tariff data from the smart meter system

3.1.9 customer energy manager (CEM)
logical entity providing functionality used to manage one or more ESAs or ESAGs, specific to a supply point, in order to provide DSR services

NOTE 1 A CEM could either be in a box located in the premises or in the cloud with connectivity to the ESA.

NOTE 2 In this PAS, the term "CEM" indicates a CEM/ESAG combination or an individual CEM, as appropriate, unless otherwise stated.

3.1.10 data communications company (DCC)
entity to establish and manage the GB data and communications network required to connect smart meters to the business systems of energy suppliers, network operators and other authorized service users of the network

NOTE Smart DCC Ltd (DCC) operates under the Smart Meter Communication Licence which was granted by the Department of Business, Energy and Industrial Strategy (BEIS) and is regulated by Ofgem.

3.1.11 demand side response (DSR)
shifting (in time) and/or modulation (increase or decrease) of electricity consumption and/or production through the controlled operation of ESAs, in line with consumer preferences, in response to signals from grid-side actors (DSRSPs or suppliers/utilities) , acting in agreement with electricity network operators and electricity system actors

3.1.12 demand side response service provider (DSRSP)
organization providing demand-side related energy management services to the operators of electricity transmission and distribution systems, and electrical energy suppliers and generators feeding energy into those systems

3.1.13 electric vehicle (EV) chargepoint
equipment enabling the recharging, or in the case of V2G discharging, of an EV

3.1.14 energy flexibility event
action of an ESA or a CEM relating to an energy flexibility request

3.1.15 energy flexibility request
request from a DSRSP to a CEM or ESA to modify load, generation or storage

3.1.16 energy gateway
communications bridge between DSR-related devices located inside and outside the premises

3.1.17 energy smart appliance (ESA)
appliance which meets the requirements specified in this PAS; it is communications-enabled and able to respond automatically to price and/or other signals by shifting or modulating its electricity consumption and/or production

3.1.18 ESA gateway (ESAG)
functional entity between one or more ESAs and a CEM

3.1.19 heating, ventilation and air conditioning (HVAC) appliances
electrical goods used in a domestic or small business environments for heating, ventilation or air conditioning

3.1.20 home area network (HAN)
communications network typically deployed over short distances and used within a premises

3.1.21 interoperability
ability of an ESA to work seamlessly across any appropriate DSR service operated by any authorized system player, including allowing a consumer to switch an ESA to a different DSRSP at any time and maintain DSR functionality

3.1.22 local physical interface
interface on the ESA or CEM that can only be accessed physically (e.g. USB port, UART, JTAG port)

3.1.23 local user interface
interface on the ESA or CEM used for user interaction that can only be accessed physically (e.g. buttons, keypad, speaker, touchpad, screen)

3.1.24 network physical interface
hardware interface that physically connects the ESA or CEM to a communications network (e.g. Ethernet, radio transceiver)

3.1.25 network logical interface
logical interface or protocol operating over the network physical interface that connects the ESA or CEM to other entities on a communications network

3.1.26 power profile

series of data points representing the value of power at points in time

3.1.27 premises
geospatial extent owned or occupied by a consumer and containing one or more appliances that consume, generate and/or store electrical energy

NOTE 1 A premises can have a mixture of energy smart and non-energy smart appliances.

NOTE 2 The appliances can be located within the buildings of the premises (for example, domestic white goods) or outside the buildings of the premises (for example, a smart EV chargepoint).

3.1.28 smart EV chargepoint
EV chargepoint that is energy smart through meeting the requirement in this PAS 1878

3.1.29 smart meter
device measuring electrical energy transfer that meets the prevailing national smart meter specification(s) for the country in which the meter is located

NOTE The current specification for GB smart meters is SMETS2.

3.1.30 smart meter home area network (SMHAN)
network used to communicate between smart meters and the “in home display”

NOTE 1 This might also be known as a smart meter display or home energy monitor and other items, e.g. smart appliances, as and when they become available.

NOTE 2 In the GB smart metering system this is a Zigbee network.

3.1.31 standalone auxiliary proportional controller (SAPC)
device controlled by the GB electricity smart metering equipment and capable of containing up to 5 APCs

3.1.32 supply point
point at which a premises connects to the electricity supply network operated by the distribution system operator (DSO) or distribution network operator (DNO)

3.2 Abbreviations

For the purposes of this PAS, the following abbreviations apply.

APC	auxiliary proportional controller
CAD	consumer access device

CA	certification authority
CEM	customer energy manager
DCC	data communications company
DNO	distribution network operator
DSO	distribution system operator
DSR	demand side response
DSRSP	demand side response service provider
ESA	energy smart appliance
ESAG	ESA gateway
EV	electric vehicle
HAN	home area network
HTTPS	secure hypertext transfer protocol
HVAC	heating ventilation and air conditioning
OCPP	open charge point protocol
OpenADR	open automated demand response
PKI	public key infrastructure
SAPC	standalone auxiliary proportional controller
SMHAN	smart meter home area network
SSL	secure sockets layer
ToU	time of use
TSO	transmission system operator
V2G	vehicle to grid
WAN	wide area network

4 ESA architecture

*COMMENTARY ON CLAUSE **4***

The ESA energy flexibility architecture is made up of functional elements. Some components some have a specified physical implementation (e.g. ESAs need to be in the presence of the consumer), whilst others are only logical with no specified physical implementation (e.g. a CEM is a logical entity, which can operate on a device in the premises or on a server for cloud-based models). Therefore, example physical implementations shown in any figures are illustrative only.

*A description of each component is provided in **4.1** to **4.3**.*

The main components associated with the systems level functional architecture are shown in Figure 3 and described in the following subclauses. This architecture is compatible with the functional architecture described in existing CENELEC and IEC documents (see BS EN 50631-1:2017, BS IEC 62746-10-1:2018, IEC TR 61850-90-8:2016 and BS EN 50491-12-1), as described in Annex F.

The Energy Smart Appliance (ESA) is a physical appliance making use of energy smart functionality and is sited on the customer premises. The CEM is a logical entity providing energy management functionality and may be sited either on the customer premises or externally to the customer premises and either as standalone equipment or as part of other equipment including the ESA itself. The DSR Service Provider (DSRSP) is a business entity logically connected to a number of ESAs via their CEMs and is sited externally to the customer premises.

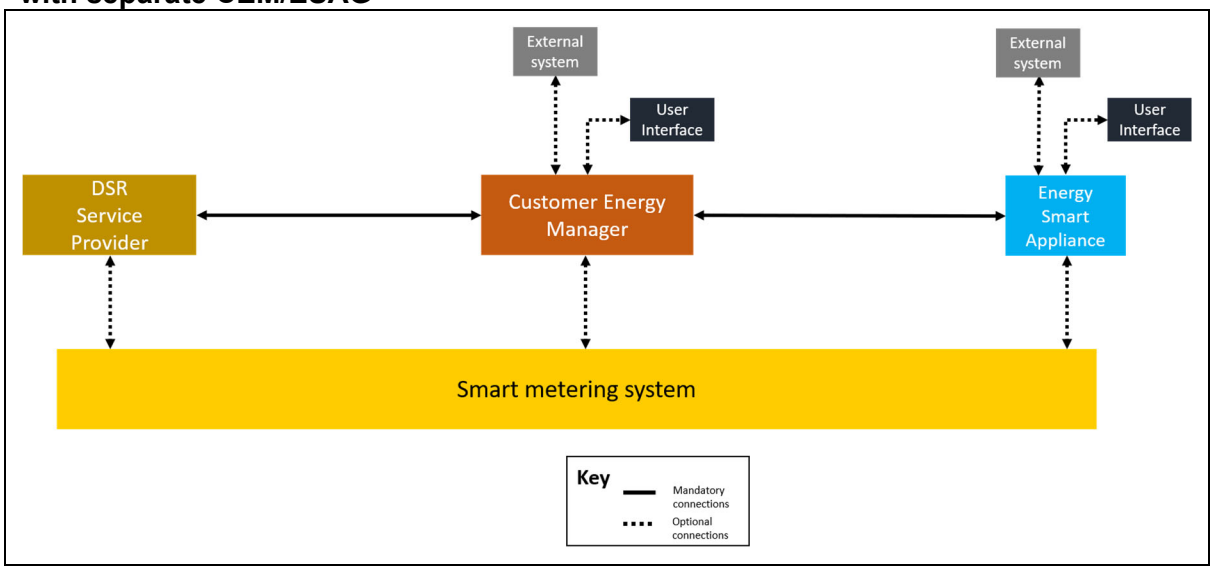
The ESA and CEM provide user interfaces for their energy smart functionality and status which allow the customer (owner or user of an ESA) to interact with the ESA, CEM and the DSR services provided by the DSRSP.

A Customer Energy Manager (CEM) is connected to only one DSR Service Provider at any one time. An Energy Smart Appliance (ESA) is connected to only one CEM at any one time. A CEM is connected to at least one ESA.

The CEM and/or the ESA might include an interface to other, non-DSR, services such as remote control applications, service and maintenance or weather forecasts. The existence, capabilities and connection with DSR services of such interfaces is determine by the manufacturer and is beyond the scope of this PAS.

ESAs can optionally communicate with a smart metering system. Smart metering systems are used to meter electricity at the grid supply point to the premises and to provide associated services. Various different implementations, with different functionalities, exist and are often country-specific. The figures show a generic representation of a smart metering system and the possible interfaces to the DSR system. Details specific to the interfacing of the GB smart metering system are described in Annex D.

Figure 3 – Representation of system level CEM–ESA energy flexibility architecture with separate CEM/ESAG



4.1 Energy smart appliance (ESA)

The operation of the ESA shall be determined by its internal control logic (see **5.3.5.1**), denoted as the appliance controller in Figure 5. The appliance controller shall send and receive information, and receive requests, across Interface B and the Manufacturer Interface via its Network Physical Interface. The appliance controller shall determine the overall operation of the ESA and shall reject any request that is not applicable (i.e. a request that would result in unsafe, detrimental or otherwise abnormal behaviour).

The ESA shall support at least one Network Physical Interface. The Network Physical Interface shall be used to support the Network Logical Interfaces described in 5.1.1 (Interfaces A and B and the Manufacturer Interface) and may/might be used to support the Network Logical Interfaces described in **5.1.2**. All Network Logical Interfaces shall be logically separate from each other.

An ESA shall send registration/authentication, power flexibility offer and status messages to its associated CEM for subsequent communication to the DSRSP. The content and availability of these messages shall be such that the CEM shall be able to losslessly apply them to Interface A, in accordance with Clauses **5** and **6**.

An ESA shall receive registration/authentication, power flexibility offer and status messages from the DSRSP via its associated CEM.

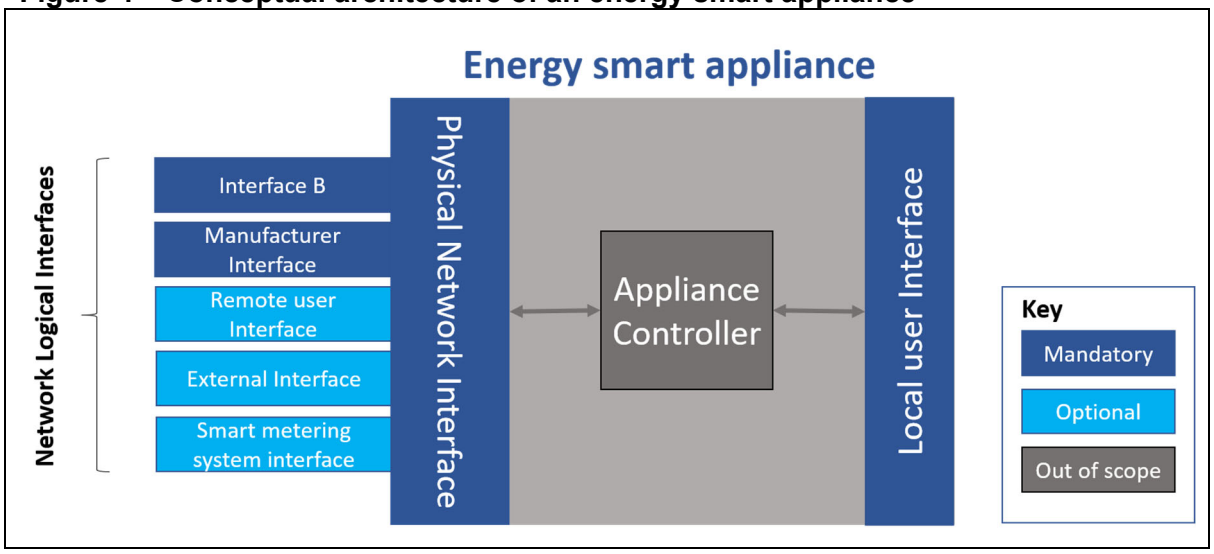
An ESA shall connect to no more than one CEM at any given time.

The ESA shall support a built-in user interface for the input of user preferences, ESA DSR operation control and the display of DSR status. The ESA may additionally support a remote user interface for the same purpose.

NOTE 1 The ESA might support other interfaces or functionality related to, for example, general configuration or maintenance. Such interfaces and functionality are beyond the scope of this PAS.

NOTE 2 The specification of the appliance controller is beyond the scope of this PAS.

Figure 4 – Conceptual architecture of an energy smart appliance



4.2 Customer energy manager (CEM)

The CEM shall act as a logical intermediary between a DSRSP and ESAs, interpreting the status of the ESA within the context of the flexibility requirements of the DSRSP, sending flexibility status information to the DSRSP and initiating ESA flexibility actions.

The CEM shall perform cyber-security operations in accordance with Clause **6** on messages that it receives from, and sends to, an ESA and DSRSP.

The CEM shall perform any reformatting or protocol transcoding on DSRSP bound messages that it receives from the ESA in order to meet the communications and message format requirements of Interface A in accordance with Clause **5**.

The CEM shall perform any reformatting or protocol transcoding on ESA bound messages that it receives from the DSRSP in order to meet the communications and message format requirements in accordance with **5.2**.

The CEM shall connect to no more than one DSRSP but shall be able to connect to at least one ESA at any given time.

NOTE 1 The CEM might allow the direct transfer of application level message payloads between the energy gateway and ESA, provided that sufficient authentication and integrity checks are performed. The CEM might be implemented on dedicated hardware, within the premises, or as a software entity, either within the premises, outside the premises or distributed across multiple platforms.

NOTE 2 The functionality of the CEM control logic is expected to satisfy a minimum set of requirements to deliver DSR services as set out in this PAS. Defining only a minimum set of requirements for DSR allows manufacturers or operators to provide value-added functionality as they see fit.

The CEM shall present one interface to the DSRSP and another to an ESA as shown in Figure 5.

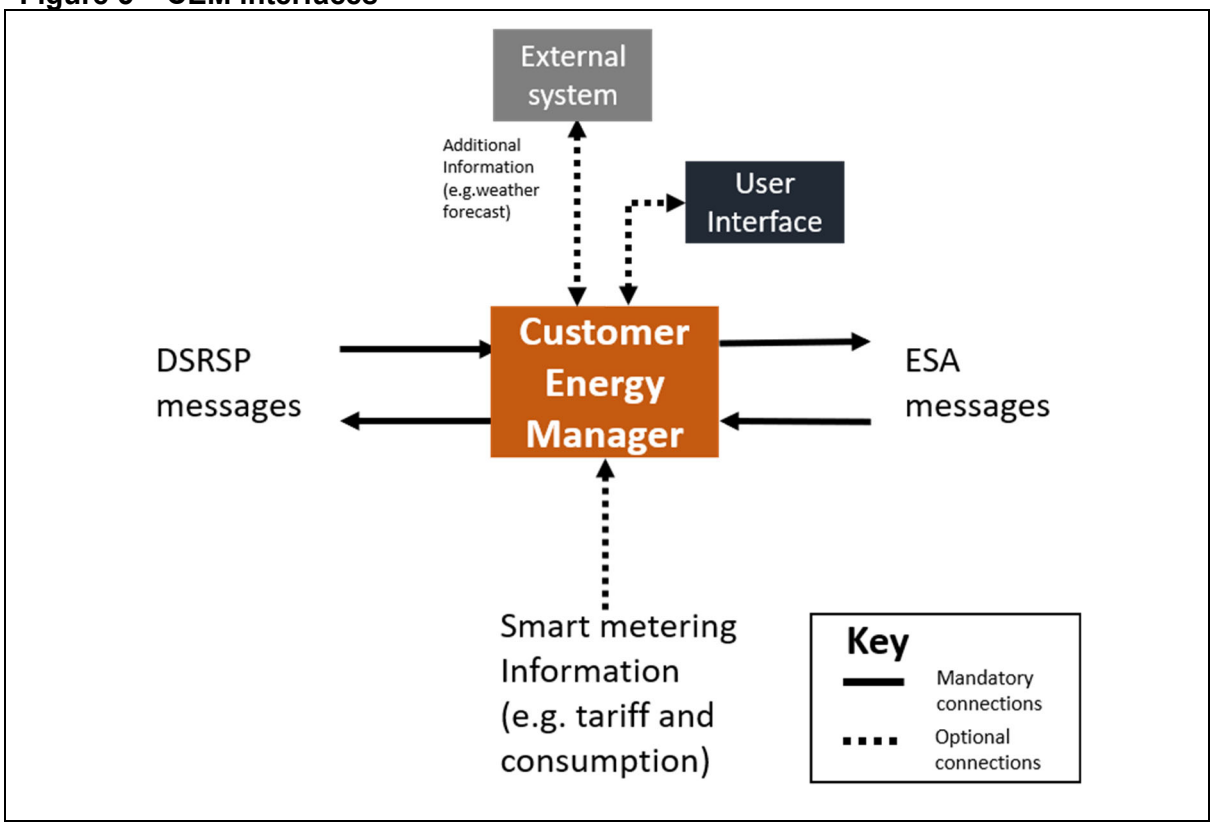
The CEM shall support either a built-in or a remote user interface for the input of user preferences and the display of DSR status.

The CEM shall operate in one of four modes, as described in **5.3.5.1**.

NOTE 3 The CEM might receive information from the smart metering system (e.g. tariff and consumption information).

*NOTE 4 The CEM might optionally support an additional interface to external systems that is used to obtain ancillary DSR-related information such as weather forecasts, to be configured and implemented such that it is at least as secure as Interface A (see Clause **5**).*

Figure 5 – CEM interfaces



4.3 Demand side response service provider (DSRSP)

The DSRSP shall be responsible for managing DSR energy flexibility amongst its subscribed CEM and ESA portfolio.

The DSRSP receives sets of power flexibility offers from each of the active CEM/ESAs in its cohort. When implementing a DSR event, the DSRSP shall select one offer from a range of sets of options and send the selection to the appropriate CEM.

The DSRSP can include the configuration of more than one organization working together, for example an aggregator working in conjunction with a third party asset manager.

The DSRSP shall present a single interface (Interface A) to each of its registered CEMs in accordance with **5.2**.

NOTE The DSRSP receives requests from grid-side actors to provide DSR services. These actors include transmission system operators, distribution system operators and optionally electricity supply organizations. The DSRSP then contacts its subscribed CEM and ESA portfolio in order to request a flexibility response as appropriate. The grid-side actors and DSRSPs, and their relationship with ESAs, is described in more detail in PAS 1879.

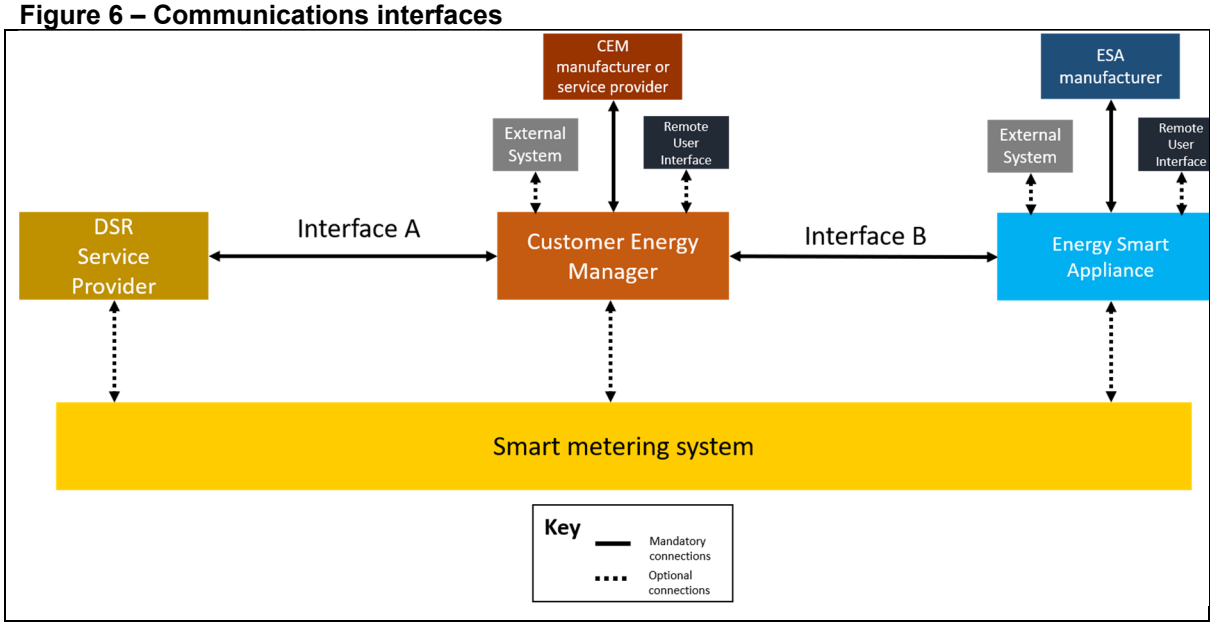
5 Communications and messaging

5.1 Interface architecture

NOTE Unless otherwise stated, references to interfaces, information and messaging shall apply to the application layer or above.

The mandatory and optional communications interfaces of the ESA DSR systems architecture are depicted in Figure 6.

Figure 6 – Communications interfaces



5.1.1 Mandatory interfaces

5.1.1.1 Interface A

The DSRSP and the CEM shall exchange information relating to device registration, de-registration, flexibility offers, DSR events, status and cyber-security breaches across Interface A. Any DSRSP shall be able to communicate with any registered CEM, and vice versa, using Interface A.

NOTE 1 Interface A is defined by this PAS in order to support interoperability between the DSRSP and the CEM, such that any DSRSP shall be able to operate with any CEM and vice versa.

This interface shall conform to the requirements described in this Clause and in Clause 6.

NOTE 2 Interface A is described in the following sections.

5.1.1.2 Interface B

The CEM and the ESA shall exchange information relating to device registration, de-registration, flexibility offers, DSR events, status and cyber-security breaches across Interface B. Interface B shall be defined by the CEM/ESA manufacturer such that there is a clear correspondence between the information model and message sequencing used by Interface A and Interface B.

The CEM shall be able to translate between the data models used on both interfaces without the loss of any information.

NOTE It is recommended that Interface B uses comparable data and message models as Interface A.

This interface shall conform to the requirements described in Clause 6.

5.1.1.3 Manufacturer interfaces

Both the CEM and the ESA shall communicate with a remote manufacturer, or service provider, portal using a logical interface defined by the manufacturer/service provider.

As a minimum, this interface shall be used to supply the CEM and ESA with firmware updates, certificate management information (new certificates, certificate revocation etc.), during the CEM and ESA mutual authentication phase described in **5.5.5** and to indicate that the CEM or ESA is to de-register.

This interface shall conform to the requirements described in Clause **6**.

5.1.1.4 User interface

A user interface shall be provided for either the CEM or the ESA (for example on a smart phone app); this interface shall conform to the requirements described in Clause **6**.

NOTE Other aspects of this interface are beyond the scope of this PAS.

5.1.2 Optional interfaces

5.1.2.1 External interfaces

Either the CEM or the ESA can connect to one or more external service providers (e.g. weather service, grid carbon intensity monitoring service) in order to provide additional functionality. When this functionality is related to DSR and energy management functionality (directly or indirectly), this interface shall conform to the requirements described in Clause **6**.

5.1.2.2 Smart metering system interface

COMMENTARY ON 5.1.2.3

The DSR system may provide for an interface or interfaces with a smart metering system. The nature and end points of the interfaces are dependent upon the DSR and smart metering systems architectures and are beyond the scope of this PAS. A description of how the DSR system could interface to the GB smart metering system is provided in Annex D ("Integration with the GB smart metering system").

This interface shall conform to the requirements described in Clause **6** as appropriate for the combination of DSR and smart metering systems.

5.2 Communications architecture

COMMENTARY ON 5.2

The logical functional architecture described in this PAS consists of an ESA within the customer premises connected through a CEM to a DSRSP in the "cloud". The CEM is a logical functional entity and so can be located within the premises or in the cloud.

Interface A shall connect the CEM and the DSRSP whether the CEM is on the premises or in the cloud.

The ESA and CEM shall communicate over Interface B using a manufacturer defined protocol. Whatever data and messaging models are used over Interface B, the CEM shall be able to translate between them and those used over Interface A in a lossless manner.

NOTE It is recommended that Interface B uses comparable data and message models to Interface A.

Regardless of the underlying communications bearer protocol (e.g. fixed broadband or mobile), it is assumed that an external CEM will use the industry standard set of Internet Protocol (IP) set of protocols for connection, cybersecurity and data transport.

In the case of an internal CEM, it is highly likely that IP (likely over ethernet) will be used over one or more bearers such as WiFi, power line or twisted pair (a cable). It is assumed that the CEM will not use a non-IP protocol set such as Zigbee 1.x for Interface A.

Interface A shall use industry standard secure internet protocols and shall support PKI.

Interface B shall support PKI and shall use a data model that is compatible with that used over Interface A.

5.3 Operation model

COMMENTARY ON 5.3

*This section describes the flow of information across the interfaces in general terms. More detail on the information model for each phase is provided in **5.4**.*

The flow of information across the interfaces is divided into the following phases:

1. *Customer registration with DSRSP*
2. *CEM and ESA mutual authentication*
3. *Device registration of the CEM and the ESA with the DSRSP*
4. *Initialization*
5. *Normal operation (4 CEM operating modes)*
6. *Exception conditions*
7. *De-registration*

5.3.1 Customer registration with DSRSP

COMMENTARY ON 5.3.1

In this phase, the Customer sets up an account with a DSRSP (possibly via a registration agent acting on behalf of the DSRSP) and is provided with information used to authenticate the ESA and CEM with the DSRSP.

The Customer shall be able to begin the registration process for the DSRSP service using a medium other than the CEM or ESA (e.g. internet portal, phone, mail or in person).

The DSRSP or registration agent shall be able to provide the Customer with information that is to be used during the CEM and ESA DSRSP service authentication and registration processes.

This information shall include:

- DSRSP authorization code;
- CEM service provision authorization code (if a remote CEM is used); and
- CEM identification token.

NOTE The details of the DSR service registration process are determined by the DSRSP and are beyond the scope of this PAS.

5.3.2 CEM and ESA mutual authentication

COMMENTARY ON 5.3.2

The necessary pre-conditions for this phase are listed in 6.3.2. The methods used to attain these pre-conditions are manufacture/service provider dependent and are beyond the scope of this PAS.

The detailed requirements for mutual CEM and ESA authentication are provided in 6.3.2.2 (CEM and ESA mutual authentication), but are summarized below.

The CEM and ESA shall mutually authenticate using PKI.

Once an authenticated connection is made between the two:

a) the CEM shall provide an identification token to the Customer (in the case of a remote CEM); or
b) the CEM shall provide an identification token to the ESA via Interface B (in the case of a local CEM).

The ESA shall send information such as its manufacturer name, serial number, EUI-64, firmware version and firmware installation date to the CEM over Interface B.

5.3.3 Registration of the CEM and the ESA with the DSRSP

The detailed requirements for the registration of the CEM and ESA with the DSRSP are provided in **6.3.2.3** (DSRSP and CEM), but are summarized below.

a) The CEM and DSRSP shall mutually authenticate using PKI over Interface A.
b) The CEM shall send its manufacturer name and serial number to the DSRSP over Interface A for validation (the DSRSP should, in response, send an identification token to the CEM over Interface A).

c) The CEM shall send its manufacturer, serial number, EUI-64, firmware version and firmware installation date to the DSRSP over Interface A.
d) The CEM shall send the ESA manufacturer, serial number, EUI-64, firmware version and firmware installation date to the DSRSP over Interface A for each ESA connected to the CEM.

Once this registration phase has been successfully completed the CEM and DSRSP shall enter the initialization phase.

5.3.4 Initialization

Once the DSRSP, CEM and ESA have successfully authenticated then they shall become associated by exchanging a set of initialization information. This information shall be exchanged during this initialization phase only.

The ESA initialization information shall be passed from the ESA to the CEM over Interface B and from the CEM to the DSRSP over Interface A.

This information shall include the flexibility offer types and the power consumption reporting types supported by the ESA.

NOTE This information might include the ESA type and classification.

The DSRSP initialization information should be passed from the DSRSP to the CEM over Interface A and, on receipt, the CEM shall pass it to the ESA over Interface B.

This information shall include the preferred power consumption reporting type.

Once the initialization phase has been successfully completed the DSRSP, CEM and ESA shall enter the normal operation phase.

5.3.5 Normal operation

During normal operation, the ESA shall:

a) inform the DSRSP, via the CEM, of its current flexibility offers;
b) inform the DSRSP, via the CEM, of any current flexibility offer updates;
c) act upon a request to implement a flexibility offer from the DSRSP, via the CEM, providing the CEM with updated profiles in response;
d) for any accepted flexibility offer requests, indicate that it is operating in a DSR event period using its user interface;
e) either periodically report its instantaneous power consumption to the DSRSP via the CEM during DSR event, or log its power consumption during a DSR event and report this to the DSRSP via the CEM as an actual power profile at the end of the DSR event;
f) send an acknowledgement for each accepted flexibility offer request to the DSRSP;
g) indicate to the DSRSP that it has cancelled the previously selected flexibility offer.

The CEM shall pass information between DSRSP and ESA, unencrypting and encrypting between Interface A and Interface B.

NOTE As part of normal operation, the DSRSP should:

a) send flexibility offer (DSR event) start requests to the ESA via the CEM;

b) send DSR event cancel requests to the ESA via the CEM;

c) request status updates from the ESA, via the CEM,

A flexibility offer (DSR event) request shall consist of an ESA flexibility offer identifier and an execution duration value .

5.3.5.1 CEM operating modes

5.3.5.1.1 General

During Normal Operation phase the CEM shall be capable of operating in any of the modes described in **5.3.5.1.2** to **5.3.5.1.6**.

5.3.5.1.2 Mode 1: Routine mode

In Mode 1, the CEM shall be able to manage the consumption/production/storage of its connected ESA(s) according to consumer preferences and other parameters (e.g. electricity tariffs, pre-programmed schedules, weather forecast, grid carbon intensity).

NOTE The CEM does not manage any current DSRSP requests in this mode.

In Mode 1, the CEM shall send ESA flexibility offer updates to the DSRSP at appropriate event points as set out in **5.3.5**.

5.3.5.1.3 Mode 2: Response mode

The CEM shall enter Mode 2 whenever it receives and is able to act upon a valid DSR request from its DSRSP (including a static or dynamic frequency response request). The CEM shall manage its connected ESA(s) according to the DSRSP request in this mode.

In Mode 2, the CEM shall send ESA flexibility offer updates to the DSRSP at appropriate event points as set out in **5.3.5**.

NOTE Dynamic and static frequency response requests should be made only to those CEM/ESA combinations that are capable of meeting the technical constraints required by the DSRSP.

If they have the capability, ESAs shall automatically invoke frequency response behaviour when mains line frequencies exceed given thresholds or deviate from given values. Such ESAs shall permit this automatic behaviour to be enabled and disabled by the DSRSP.

The CEM shall remain in Mode 2 until:

- the period stated by the DSRSP request ends;
- the DSRSP requests the period to end; or
- the consumer overrides the DSR operation; or
- the failsafe protections occur.

5.3.5.1.4 Mode 3: Consumer override

The CEM shall enter Mode 3 whenever it receives a manual override from the consumer.

In Mode 3, the CEM shall allow the consumer to override (i.e. modify, decline or cancel) any routine or response mode operation at any time. This shall be in addition to any existing preferences set by the consumer which are used in the construction of flexibility offering options for routine and response mode. The override shall be one of:

a) modification of a planned flexibility offering or current flexibility option;

b) rejection of a requested operation;

c) cancellation of all routine and/or response mode operations for a specific interval; or

d) cancellation of an ongoing routine or response mode operation.

5.3.5.1.5 Mode 4: ESA failsafe

The ESA shall include control logic (the appliance controller) that ensures the ESA does not perform in a manner that can lead to an unsafe, harmful or otherwise hazardous situation, by putting the ESA into a failsafe state. The ESA shall notify the CEM when this control logic puts the ESA into a failsafe state.

The CEM shall enter Mode 4 whenever it receives notification from the ESA that it is in a failsafe state.

Although the DSRSP and CEM should not request an ESA to perform an operation that would result in unsafe, hazardous or otherwise harmful operation, ultimately the ESA's control logic shall ensure that the ESA operates in a safe manner at all times, by putting the ESA into a failsafe state.

5.3.5.2 CEM operating mode priority

The operating modes of the CEM and ESA shall be prioritized as specified in Table 1, where the highest priority is Priority 1st.

Table 1 – Operating modes

Priority	Operating mode
1st	ESA failsafe
2nd	Consumer override A)
3rd	Response mode B)
4th	Routine mode

A) The consumer sets their preferences, which will be automatically considered in Routine and Response Modes. This case specifies a subsequent manual intervention to override planned operation.

B) This might be forecast power profiles, curtailment power values over a given period or frequency response services, depending on the capabilities of the individual ESA.

5.3.6 Exception conditions

The ESA shall:

a) notify the DSRSP and the CEM of any attempt by unauthorized parties to compromise its operation or to access sensitive information (see **6.7.2**) and;
b) determine if an exception condition has occurred and, if so, transition to the "exception" state, inform the CEM and indicate its condition using its local user interface.

The CEM shall:

a) notify the DSRSP and the ESA of any attempt by unauthorized parties to compromise its operation or to access sensitive information (see **6.7.2**)

b) determine if an exception condition has occurred and, if so, transition to the "exception" state, inform the DSRSP and ESA and indicate its condition using its local user interface; and

c) pass any information relating to ESA exceptions to the DSRSP.

NOTE In such a situation, the DSRSP should:

a) notify its cohort of ESAs, via their CEMs, of any attempt by unauthorized parties to compromise its operation or to access sensitive information; and

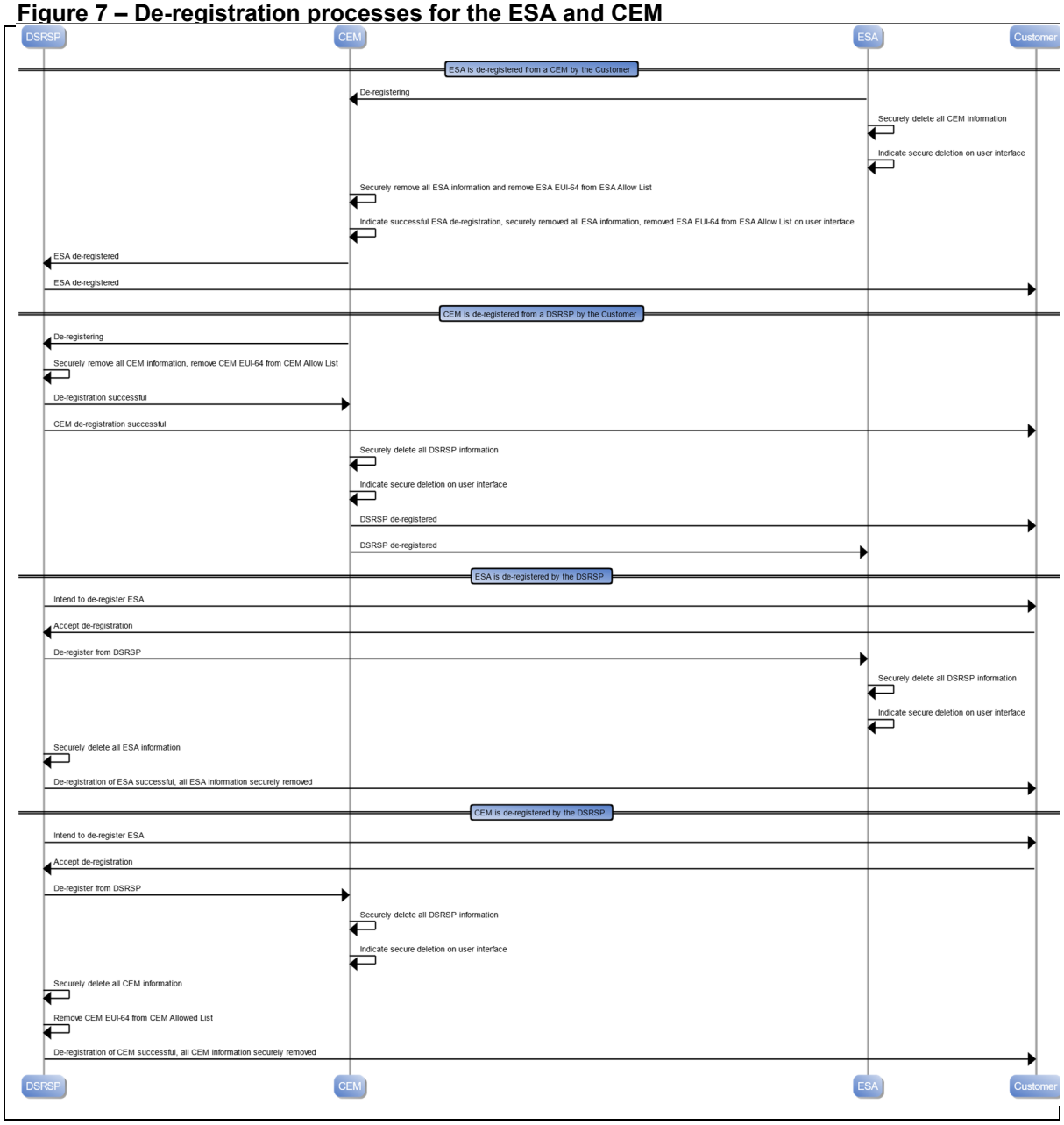
b) determine if an exception condition has occurred and, if so, transition to the "exception" state, inform its cohort of ESAs, via their CEMs, and indicate its condition using its user interface.

5.3.7 De-registration

COMMENTARY ON 5.3.7

The de-registration processes described below are illustrated in Figure 7.

Figure 7 – De-registration processes for the ESA and CEM



5.3.7.1 De-registration by customer

When an ESA is instructed to perform the “de-registration mode”/ and “de-register from CEM” operation, the ESA shall send a “de-register request” message to the CEM. The CEM shall await confirmation from the Customer before sending a “de-registration confirmation” message to the ESA. The ESA shall securely remove all information related to the CEM and DSRSP, logging all actions before informing that Customer that its information removal process is complete.

The CEM shall securely remove all information related to the CEM and DSRSP, logging all actions, before sending an “ESA de-registration notification” message to the DSRSP.

The DSRSP shall securely remove all information related to the ESA and log all actions before sending an “ESA de-registration acknowledged” message to the CEM.

The CEM shall inform the Customer that the ESA de-registration process is complete and that ESA information has been removed from the DSRSP.

NOTE 1 The DSRSP should indicate to the Customer that the ESA has been de-registered.

When a CEM is being de-registered from a DSRSP by the Customer, the CEM shall send a "de-registering" message to the DSRSP. On receipt of a "de-registration successful" message from the DSRSP to the CEM and to the Customer, the CEM shall then securely delete all information associated with the DSRSP and shall indicate on its user interface that all information associated with the DSRSP has been securely deleted. The CEM shall indicate to the Customer and to the ESA that it has been de-registered from the DSRSP.

NOTE 2 When an ESA is being de-registered by the DSRSP, the DSRSP should inform the customer that the ESA is being de-registered and await confirmation before the de-registration process is initiated.

The ESA shall securely remove all DSRSP information and indicate successful removal on its user interface.

NOTE 3 The DSRSP should securely remove all ESA information and inform the Customer of successful de-registration).

5.3.7.2 De-registration by the DSRSP

When a CEM is being de-registered by the DSRSP, the CEM shall securely remove all DSRSP information and indicate successful removal on its user interface.

NOTE The DSRSP should inform the customer that the CEM is being de-registered and await confirmation before the de-registration process is initiated. When the CEM has removed all DSRSP information, the DSRSP should securely remove all corresponding CEM information and remove the CEM EUI-64 from its CEM Allowed List. The Customer should be informed of successful information removal and de-registration.

5.4 Information model

COMMENTARY ON 5.4

*This section describes the flow of information across the interfaces in detail, the detailed information elements facilitate the operation model in **5.3**.*

The flow of information across the interfaces is divided into the following phases:

1. *Customer registration with DSRSP (excluded from information model)*
2. *CEM and ESA mutual authentication*
3. *Registration of the CEM and the ESA with the DSRSP*
4. *Initialization*
5. *Normal operation (four CEM operating modes)*
6. *Exception conditions*
7. *De-registration*

A DSRSP and CEM shall act upon and generate all the information listed below in **5.4.1** and **5.4.2** in order to be compliant with Interface A. The information listed below shall form the basis of a data model.

This data model might be formatted to conform to OpenADR or EEBus, see Note in **5.7**. Comments welcome.

An ESA shall act upon all information listed below in **5.4.2** generated by the DSRSP and shall generate the information listed below that corresponds to the capabilities of the ESA (e.g. only those flexibility offer types that the ESA supports).

The ESA shall exchange information with the CEM over Interface B. The CEM shall exchange information with the DSRSP over Interface A. The CEM shall perform any translation between the data format used over Interface A and Interface B. This translation shall use the Interface A data model as a reference.

The Interface B data model shall be designed such that the translation performed by the CEM results in no loss of information.

5.4.1 CEM and ESA mutual authentication

5.4.1.1 Information passed from ESA to the CEM

The information in Table 2 shall be passed from the ESA to the CEM in addition to that used for the PKI authentication process.

Table 2 – Information passed from the ESA to the CEM during the mutual authentication process

Information element	Mandatory/optional	Note
ESA manufacturer name	M	
ESA unique serial number	M	
ESA EUI-64	M	
ESA firmware version	M	
ESA firmware update date	M	

5.4.1.1.1 ESA Manufacturer

This information element shall provide the name of the ESA manufacturer.

NOTE The manufacturer's Operator User Interface could be used rather than the name as a string.

5.4.1.1.2 ESA serial number

This information element shall provide the unique serial number of the ESA.

5.4.1.1.3 ESA EUI-64

This information element shall provide the Extended Unique Identifier of the ESA [this is an 8 byte (64 bit) value].

5.4.1.1.4 ESA Firmware version

This information element shall provide the version of the most recently installed firmware (this is used to check for known functional or security issues and as an input into identity validation).

5.4.1.1.5 ESA Firmware update date

This information element shall provide the installation date of the most recently installed firmware (this is used as an input into identity validation).

5.4.1.2 Information passed from the CEM to the ESA

The information in Table 3 shall be passed from the CEM to the ESA in addition to that used for the PKI authentication process.

Table 3 – Information passed from the CEM to the ESA during the mutual authentication process

Information element	Mandatory/optional	Note
Identification token	M	String. Local CEM only

5.4.1.2.1 Identification token

This information element shall be sent from the local CEM to the ESA as part of the authentication verification process. For the external CEM case, this token shall be passed to the Customer and is not passed over Interface A or B.

5.4.2 Registration of the CEM and the ESA with the DSRSP

5.4.2.1 Information passed from the CEM to the DSRSP

The information in Table 4 shall be passed from the CEM to the DSRSP, in addition to that used for the PKI authentication process (as described in **6.3.2.3**), in order to allow the CEM and ESA to be registered with the DSRSP.

Table 4 – Information passed from the CEM to the DSRSP during the CEM/ESA registration process

Information element	Mandatory/optional	Note
CEM manufacturer name	M	
CEM unique serial number	M	
CEM EUI-64	M	
CEM firmware version	M	
CEM firmware update date	M	
ESA manufacturer name	M	
ESA unique serial number	M	
ESA EUI-64	M	
ESA firmware version	M	
ESA firmware update date	M	

5.4.2.1.1 CEM Manufacturer

This information element shall provide the name of the CEM manufacturer.

NOTE The manufacturer's Operator User Interface could be used rather than the name.

5.4.2.1.2 CEM serial number

This information element shall provide the serial number of the CEM.

5.4.2.1.3 CEM EUI-64

This information element shall provide the Extended Unique Identifier of the CEM. This shall be an 8 byte (64 bit) value.

5.4.2.1.4 CEM Firmware version

This information element shall provide the version of the most recently installed firmware (this is used to check for known functional or security issues and as an input into identity validation).

5.4.2.1.5 CEM Firmware update date

This information element provides the installation date of the most recently installed firmware (this is used as an input into identity validation).

5.4.2.2 Information passed from the DSRSP to the CEM

The CEM shall be able to receive the information in Table 6 from the DSRSP, in addition to that used for the PKI authentication process (as described in **6.3.2.2**), in order to allow the CEM and ESA to be registered with the DSRSP.

Table 5 – Information passed from the CEM to the ESA during the mutual authentication process

Information element	Mandatory/optional	Note
Identification token	M	String. Local CEM only

5.4.2.2.1 Identification token

The CEM shall receive and process this information element, when sent from the DSRSP over Interface A as part of the authentication verification process.

5.4.3 Initialization

5.4.3.1 Information passed from the ESA to the DSRSP via the CEM

The information in Table 6 shall be passed from the ESA to the DSRSP, via the CEM, in order to inform the DSRSP of ESA properties relating to the Normal operation phase. This information shall be exchanged during this initialization phase only.

Table 6 – Information passed from the ESA to the DSRSP via the CEM during initialization

Information element	Mandatory/optional	Note
Flexibility offer types	M	Forecast power profile, curtailment, frequency response
Power reporting type	M	Periodic power update (with max. update frequency), actual power profile
ESA type	O	(HVAC, EV charger, etc.)
ESA classification	O	Max/min consumption and/or production

5.4.3.1.1 Flexibility offer type

This information element shall be used to inform the DSRSP which flexibility offer types the ESA is capable of providing during Normal operation, and shall consist of one or more of the following:

- forecast power profiles;
- curtailment power values over a given period and;
- frequency response services.

5.4.3.1.2 Power reporting type

This information element shall be used to inform the DSRSP of which type of power consumption/production reporting the ESA is capable of providing, and shall consist of at least one of the following:

- instantaneous power consumption or production (provided as a frequency value), sent to the DSRSP with a given periodicity defined by the frequency value; and
- power consumption or production profile (a set of arrays of power consumption values), sent to the DSRSP following the end of a DSR event.

5.4.3.1.3 ESA type

The ESA type information element is optionally used to indicate the type of ESA, which shall consist of one of the following:

- electric HVAC;
- cold appliance;
- wet appliance;
- battery storage; or
- smart EV chargepoint.

5.4.3.1.4 ESA classification

The ESA classification information element shall indicate the maximum and minimum consumption and/or production power of the ESA; this information within the element is optional.

5.4.3.2 Information passed from the DSRSP to the ESA via the CEM

The ESA shall be able to receive and process the information shown in Table 7 from the DSRSP(via the CEM) in order to inform it of DSRSP preferences relating to the Normal operation phase. This information shall be exchanged during this initialization phase only.

Table 7 – Information passed from the DSRSP to the ESA via the CEM during initialization

Information element	Mandatory/optional	Note
Preferred power reporting type	M	Provided only if the ESA presents a choice to the DSRSP

5.4.3.2.1 Preferred power reporting type

The preferred power reporting type information element shall be provided to the ESA by the DSRSP If the ESA is capable of supporting more than one power reporting type.

5.4.4 Normal operation

5.4.4.1 Information passed from the ESA to the DSRSP via the CEM

The information in Table 8 shall be passed from the ESA to the DSRSP, via the CEM, as necessary during Normal operation phase.

Table 8 – Information passed from the ESA to the DSRSP via the CEM during normal operation

Information element	Mandatory/optional	Note
Flexibility offers	M	
Actual power profile	M	M only if type supported or selected by DSRSP
Actual instantaneous power value	M	M only if type supported or selected by DSRSP
Acknowledgements	M	
DSR event cancelled	M	
Free text	O	DSRSP specific

5.4.4.1.1 Flexibility offers

The ESA shall inform the DSRSP about its current flexibility offerings using this information. This information shall include the following:

- forecast power profiles – at least the minimum required set of “least delayed”, “intended operation” and “most delayed” forecast power profiles; and
- frequency response service – indicating the ESA is able to move into a frequency response mode for a specified period, following a message from the DSRSP. The state of this element shall indicate the frequency response capability of the ESA and is associated with a forecast power profile.

All flexibility offer messages shall include an ESA flexibility offer identifier in order to allow the DSRSP to identify the particular offer in any subsequent flexibility offer request messages. Any active ESA flexibility offer identifier values shall be distinct.

NOTE An active offer shall be one that has been sent to, and is currently considered for implementation by, the DSRSP.

5.4.4.1.2 Actual power profile

If the ESA is able to provide actual power profiles to the DSRSP or if the DSRSP has selected this reporting type during the Initialization phase, then the ESA shall provide actual power profiles following the end of each DSR event.

The requirements in **5.5.7** shall be met for actual instantaneous power value reporting.

5.4.4.1.3 Actual instantaneous power value

If the ESA is able to provide instantaneous power values to the DSRSP, or if the DSRSP has selected this reporting type during the Initialization phase, then it shall do so at a frequency indicated in the “power reporting type” initialization information element (see **5.4.3.2**).

The requirements in **5.5.7** shall be met for actual instantaneous power value reporting.

5.4.4.1.4 Acknowledgements

The ESA shall indicate its implementation one of its flexibility offerings as chosen by the DSRSP by sending an acknowledgement to the DSRSP.

NOTE This allows both the ESA and the DSRSP to keep a log of the notified flexibility offerings requested by the DSRSP and provided by the ESA.

5.4.4.1.5 DSR event cancelled

The “DSR event cancelled” information element shall be used by the ESA to indicate to the DSRSP that it is no longer implementing the previously selected flexibility offer.

5.4.4.1.6 Free text

Where information is provided that is beyond the scope of Interface A, free text shall be used.

NOTE In some cases, the ESA manufacturer might be able to provide additional information to the DSRSP, as specified by the DSRSP. This information might be beyond the scope of Interface A.

5.4.4.2 Information passed from the DSRSP to the ESA via the CEM

The CEM and ESA shall be able to receive and process the following information (depicted in Table 9), when sent by the DSRSP over Interface A.

Table 9 – Information passed from the DSRSP to the ESA during normal operation

Information element	Mandatory/optional	Note
Flexibility offer request	M	Format depends upon flexibility offer type. Includes execution duration value. Includes optional “communications timeout” value and “wait for start” indicator.
DSR event cancelled	M	Includes cancelled flexibility offer identifier
Tariff	O	Country/supplier-specific format

5.4.4.2.1 Flexibility offer request

The flexibility offer request information element is used by the DSRSP to indicate which current ESA flexibility offer it is requesting the ESA to perform; this information element shall include the ESA flexibility offer identifier and an execution period (the duration of which shall be less than or equal to the remaining duration available for the flexibility offer).

NOTE If the ESA reports that it is capable of performing frequency response in the corresponding flexibility offer then the flexibility offer request should include maximum frequency and minimum frequency limits.

This information element might include a “communications timeout” value: during a DSR Event related to the flexibility offer request, when an ESA experiences communications failure, it shall start a timer. When this timer reaches either the value “communications timeout” or the execution duration value whichever comes first, then the ESA shall cancel the current DSR Event operation and return to non-DSR operation (Routine mode).

5.4.4.2.2 DSR event cancelled

The “DSR event cancelled” information element is used by the DSRSP to signal to the appropriate ESA that the ESA should cancel the current DSR event: this information element shall include the ESA flexibility offer identifier.

5.4.5 Exception conditions

5.4.5.1 Information passed from the ESA to the CEM and DSRSP

The information in Table 10 shall be passed from the ESA to the DSRSP and CEM whenever exception conditions arise.

Table 10 – Information passed from the ESA to the CEM to the DSRSP to indicate exception conditions

Information element	Mandatory/optional	Note
Attempt to compromise ESA	M	Includes exception code

5.4.5.1.1 Attempt to compromise ESA

This information element shall be passed by the ESA to the CEM and the DSRSP to indicate that it has suffered an exception condition. The information element shall include the ESA EUI-64 and an exception condition code.

5.4.5.1.1 1 Exception condition code

Exception conditions shall be represented by the list in Table 11. The information element shall include the appropriate code.

Table 11 – Exception condition codes

Exception condition	Code
Unauthorized attempt to access interfaces	1
Unauthorized attempt to physically compromise device	2
Inappropriate flexibility request received	3
Malware detected	4

5.4.5.2 Information passed from the CEM to the DSRSP and ESA

The following information, shown in Table 12, shall be passed from the CEM to the CEM and DSRSP whenever exception conditions arise.

Table 12 – Information passed from the CEM to the DSRSP and ESA to indicate exception conditions

Information element	Mandatory/optional	Note
Attempt to compromise CEM	M	Includes exception code

5.4.5.2.1 Attempt to compromise CEM

This information element shall be passed by the CEM to the ESA and the DSRSP to indicate that it has suffered an exception condition. The information element shall include the CEM EUI-64 and an exception condition code.

5.4.5.2.2 Exception condition code

Exception conditions shall be represented by the list in Table 13. The information element shall include the appropriate code.

Table 13 – Exception condition codes

Exception condition	Code
Unauthorized attempt to access interfaces	1
Unauthorized attempt to physically compromise device	2
Inappropriate flexibility request received	3
Malware detected	4

5.4.5.3 Information passed from the DSRSP to the CEM and ESA

The CEM and ESA shall be able to receive and process the information in Table 14, when passed over Interface A by the DSRSP. whenever exception conditions arise.

Table 14 – Information passed from the ESA via the CEM to the DSRSP to indicate exception conditions

Information element	Mandatory/optional	Note
Attempt to compromise DSRSP	M	Includes exception code

5.4.5.3.1 Exception condition code

Exception conditions shall be represented by the list in Table 15. The information element shall include the appropriate code.

Table 15 – Exception condition codes

Exception condition	Code
Unauthorized attempt to access interfaces	1
Unauthorized attempt to physically compromise device	2
Inappropriate flexibility offers received (include ESA EUI-64)	3
Malware detected	4

5.4.6 De-registration

5.4.6.1 Information passed from the ESA to the CEM and DSRSP

The information in Table 16 shall be passed from the ESA to the CEM and DSRSP whenever the ESA wishes to de-register from the DSRSP.

Table 16 – Information passed from the ESA to the CEM to the DSRSP to indicate de-registration

Information element	Mandatory/optional	Note
ESA de-registration	M	

5.4.6.1.1 ESA de-registration

This shall be an indication from the ESA that the CEM and DSRSP shall remove it from their registration lists.

Whenever the CEM receives this information element from the ESA, the CEM shall perform the operations defined in **5.3.7**.

5.4.6.2 Information passed from the CEM to the ESA and DSRSP

The information in Table 17 shall be passed from the CEM to the ESA and DSRSP whenever the CEM wishes to de-register from the DSRSP.

Table 17 – Information passed from the CEM to the ESA and the DSRSP to indicate de-registration

Information element	Mandatory/optional	Note
CEM de-registration	M	

5.4.6.2.1 CEM de-registration

This shall be an indication from the CEM that the ESA and DSRSP shall remove it from their registration lists.

5.5 DSR flexibility offers and power information

5.5.1 General

In order to allow the DSRSP to maintain an up-to-date view of the flexibility offers available to it, each CEM shall provide the DSRSP with information relating to the flexibility offers provided by its ESAs.

These flexibility offers shall consist of forecast power profiles (see **5.5.2**), or frequency response service (see **5.5.5**).

In order to allow the DSRSP to provide the required response during a DSR event, each CEM shall provide the DSRSP with information relating to the actual power values or profiles provided by its ESAs (see **5.5.4**).

5.5.2 Forecast power profiles

The ESA and CEM shall provide a set of indexed forecast power profiles to the DSRSP whenever the status changes for any of the minimum required set of power profiles.

NOTE 1 A status change occurs when any of the following occur:

- *consumer intervention, or optional external data update;*
- *start of any active period in any profile (IO, MD, LD);*
- *end of any active period in any profile (IO, MD, LD).*

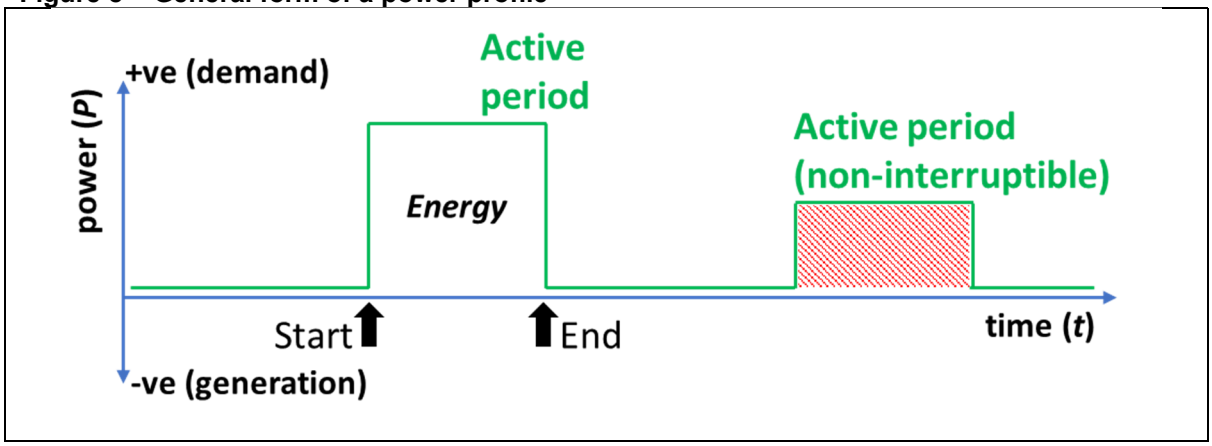
NOTE 2 In order to minimize the number of updates required, this event-triggered update approach is specified as opposed to an approach of providing updates continuously at regular intervals.

The CEM or ESA shall be able to receive messages from the DSRSP, stating which flexibility offer it wishes to initiate, based on the power profile (ESA flexibility offer identifier) it has selected.

5.5.3 Use of profiles

The ESA shall indicate its flexibility capability by generating a set of indexed forecast power profiles each with an associated ESA flexibility offer identifier. These shall be passed to the CEM, where they shall be logged. In addition, an identifier linking the forecast to the particular ESA shall be appended to the ESA forecasts. The general form of a power profile is show in Figure 5.3.

Figure 8 – General form of a power profile



The ESA shall send an updated set of forecast power profiles whenever the status changes and these shall be forwarded to the DSRSP.

NOTE 1 The DSRSP is then able to build up a model of the forecast flexibility options offered to it at any given time by its cohort of premises or ESAs.

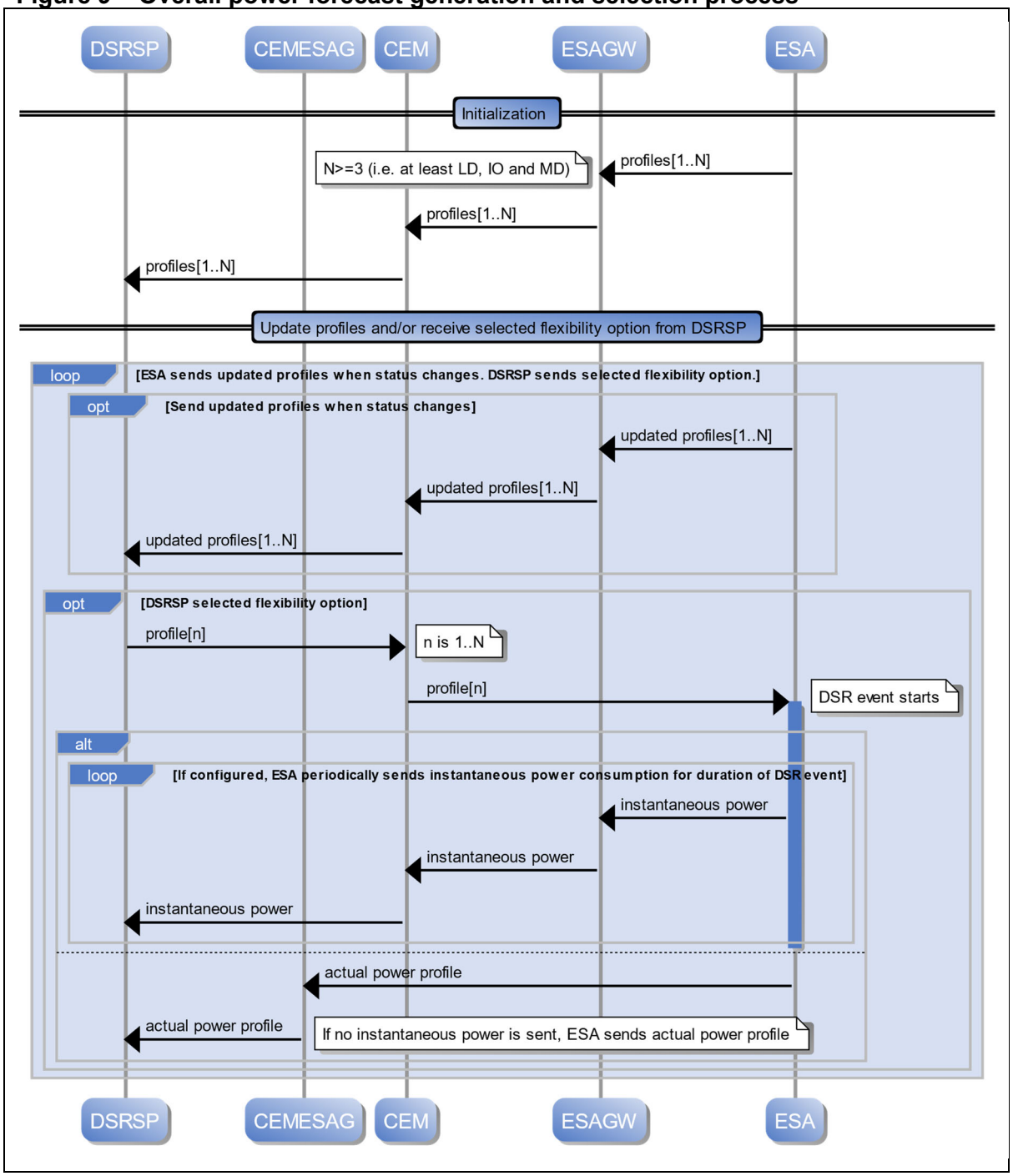
NOTE 2 When the DSRSP wishes to initiate a DSR event period, it should determine the flexibility options available to it by examining the forecast power profiles, and select one. The DSRSP should then send a message including the index of the chosen forecast to the appropriate CEM.

The CEM shall log all requests coming from the DSRSP.

The ESA shall provide power consumption information to the DSRSP during the DSR event. This shall be performed either by periodically sending instantaneous actual power values during the DSR event or by sending a log of the period power values (as an “actual power profile”) immediately after the DSR event.

NOTE 3 The overall process is illustrated in Figure 5.4.

Figure 9 – Overall power forecast generation and selection process



5.5.4 Minimum set of forecast power profiles

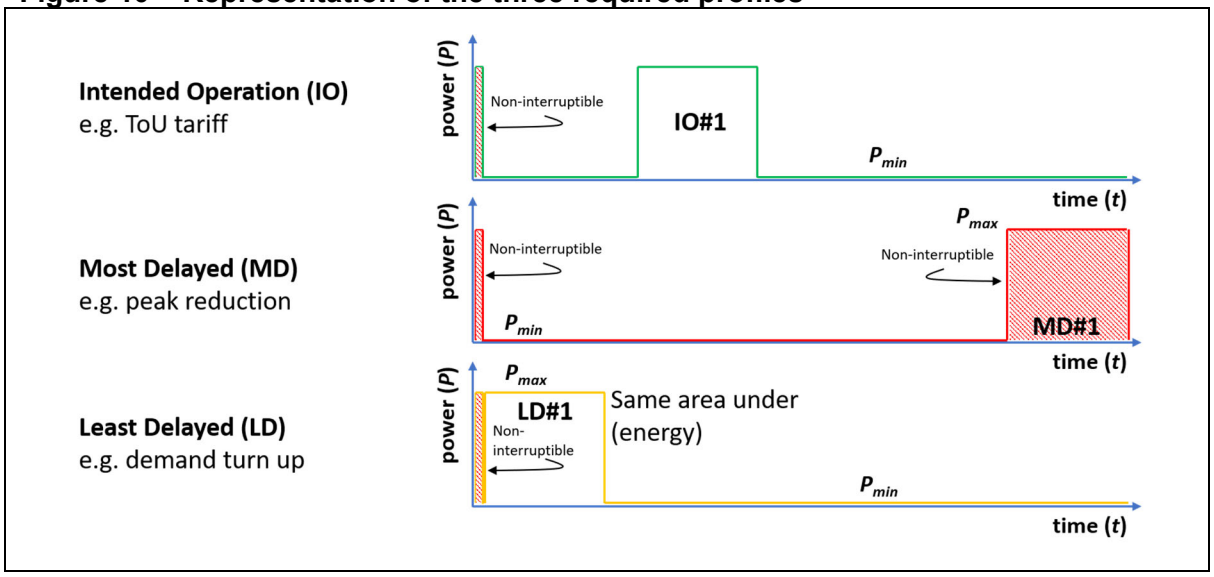
5.5.4.1 General

The ESA shall generate at least three forecast power profiles:

- intended operation (IO);
- most delayed (MD); and
- least delayed (LD).

NOTE An example of these three profile types is shown in Figure 5.5.

Figure 10 – Representation of the three required profiles



ESAs able to produce power, such as battery storage, shall also generate two additional forecast power profiles:

- most delayed production;
- least delayed production.

5.5.4.2 Intended operation

The “intended operation” (IO) power profile shall correspond to the operation of the ESA when not responding to a flexibility offer request from a DSRSP. This shall include expected behaviour according to consumer preferences and optionally the local energy environment, e.g. ToU tariff, local generation, minimum carbon, etc. An ESA shall provide an IO profile on initiation of the ESA and whenever the IO profile changes.

This profile shall have the capacity to contain interruptible and non-interruptible segments.

5.5.4.3 Most delayed

The “most delayed” (MD) power profile shall correspond to the latest time at which an ESA is able to start whilst still meeting the requirements of the consumer in providing the service. An ESA shall provide an MD profile on initiation of the ESA and whenever the MD profile changes. This profile shall be non-interruptible.

5.5.4.4 Least delayed

The “least delayed” (LD) power profile shall correspond to the earliest time at which an ESA is able to start whilst still meeting the requirements of the consumer in providing the service. An ESA shall provide an LD profile on initiation of the ESA and whenever the LD profile changes. This profile shall have the capacity to contain interruptible and non-interruptible segments.

5.5.4.5 Incorporating randomized offsets in power profiles

To avoid large simultaneous unwanted switches in load on the electricity network, the CEM/ ESA shall be developed with functionality to offer randomized offsets of up to 30 minutes.

When the CEM/ESA creates the Intended Operation power profiles, the CEM/ ESA shall incorporate randomized offsets, if these are not already included (e.g. included in ToU tariffs with built-in randomized offsets). The randomized offset shall be between 0 and 10 minutes.

The consumer override function specified in **5.3.5.1.4** shall be able to override the randomized offset, if activated by the consumer.

The CEM/ESA shall not incorporate randomized offsets when creating the Most Delayed and Least Delayed power profiles, as these will be used to provide fast-responding DSR services.

5.5.4.6 Use of the required forecast power profile types

Considering the message flow shown in Figure 9 and the example forecast power profiles shown in Figure 10:

- the ESA shall calculate the initial IO, MD and LD forecast power profiles for a given flexibility forecast period;
- these shall be sent to the DSRSP via the CEM whenever their status changes or they expire;
- following the beginning of the flexibility forecast period, the ESA shall send updates for the IO, LD and MD forecast power profiles as they change with time and ESA status; and
- upon requesting a DSR event, the DSRSP can select either LD or MD as it sees fit and send the request to the CEM and/or ESA, which shall respond as quickly as possible, either accepting the DSRSP's request or rejecting it.

5.5.5 Frequency response flexibility offers

If they have the capability, ESAs shall be capable of automatically invoking frequency response behaviour when mains line frequencies exceed given thresholds or deviate from given values. Such ESAs shall permit this automatic behaviour to be enabled and disabled by the DSRSP. If an ESA is capable of frequency response flexibility then it shall indicate its current capability by sending a frequency response flexibility offer to the DSRSP via the CEM.

The ESA shall include a frequency response capability indicator in the frequency response flexibility offer, in addition to the information defined in **5.4.4.1.1**

The frequency response capability indicator shall be defined as follows:

- 0 indicates that it is not frequency response capable;
- 1 indicates it is static frequency response capable;
- 2 indicates it is dynamic frequency response capable with a response linearly proportional to the frequency deviation;
- 3 indicates it is dynamic frequency response capable with a response proportional to the square of the frequency deviation;
- N indicates it is dynamic frequency response capable with a response proportional to (N-1)th power of the frequency deviation.

The ESA shall provide frequency response offer updates to the DSRSP, via the CEM, whenever the ESA frequency response status changes.

5.5.6 Frequency response offer request

If capable, the CEM or ESA shall be able to receive requests from the DSRSP including the frequency response offer request message resulting from a frequency response flexibility offer to the DSRSP.

In addition to the ESA flexibility offer identifier, the frequency response offer request message shall include frequency information: that is, maximum frequency limit and minimum frequency limit, for which:

- 0 indicates "do not implement" frequency response capability; and

- A maximum frequency limit equal to minimum frequency limit indicates a target frequency to aim for e.g. 50Hz.

NOTE For battery storage, requests might include both the consumption and production power profiles to allow high and low frequency excursions to be mitigated over the DSR Event duration

5.6 Actual power value or profile provision

An ESA shall be capable of measuring or calculating its power consumption/production value in kW (e.g. by using an internal meter or using a look-up table).

An ESA shall be capable of measuring or calculating its power consumption/production values every 1 s.

An ESA shall be capable of measuring or calculating its power consumption/production values with an accuracy upper limit of 10% standard deviation error on reported power values.

Manufacturers shall ensure errors in ESA reported power values are randomly distributed around the true value and shall ensure a normal distribution of errors for the ESA reported power values.

NOTE 1 In the UK there is currently no regulatory or legal requirement specifically on metering DSR provision. There are regulatory and legal requirements on metering electricity supply for consumer consumption settlement In this case the approach must be compliant with Schedule 7 of the Electricity Act 1989 covering Use, etc of Electricity Meters and The Measuring Instruments Regulations SI 2016/1153. In the UK the Balancing and Settlement Code defines Codes of Practice which provide further details on metering requirements, see https://www.elexon.co.uk/bsc-and-codes/bsc-related-documents/codes-of-practice/.

NOTE 2 The DSRSP needs to report back to its grid side client the DSR response that has been enacted using a cohort of N individual ESAs. If the error in the power measurement of the N devices is normally distributed and random, the accuracy of the total power change achieved is improved by the square root of N. As an example, 10 000 ESAs supplying a power response of 1kW each, with a measurement accuracy of 10%, will allow the total response of 10MW to be reported to the grid side client to an accuracy of 0.1%.

An ESA shall make the following data available over Interface B:

- instantaneous power consumption/production;
- historic power consumption/production; and
- historic power consumption/production profiles over the period of a DSRSP request.

An ESA shall notify the DSRSP of its power reporting capability.

An ESA shall report its instantaneous power consumption/production values periodically to the DSRSP during Response mode, the periodicity being negotiated between the DSRSP and ESA.

The ESA shall measure or calculate and report the power consumption/production values to meet the particular requirements of the DSRSP. These requirements are based on the DSR service provided, illustrative examples of DR services are shown in **Table C.2**.

The ESA shall be able to provide the Consumer with information comparing the actual power profile during a flexibility event with the intended profile during a flexibility event.

The ESA shall be able to provide the CEM with information comparing the actual power profile during a flexibility event with the DSRSP requested profile during the flexibility event.

5.7 Data model, messaging sequence and communication protocols

The final PAS will specify a minimum data model, message sequencing and underlying communications protocols, that meet the requirements in this Clause, for Interface A in order to support interoperability between the DSRSP and CEM. Furthermore, this interoperable Interface A definition shall meet the cyber-security requirements described in Clause 6.

Annexes G and H have been included in this PAS in order to provide summaries of two such candidate approaches – OpenADR and EEBus. The PAS could specify one or both of these approaches for Interfaces A, or it could specify a different approach. The DSRSP will need to support all specified approaches (e.g. EEBus and OpenADR) whereas the CEM will need to support only one approach.

The reader is requested to provide their choice and reasons for a preferred option, including a new option, and further invited to provide comments on the benefits, barriers and risks for each option.

6 Cyber security

*COMMENTARY ON CLAUSE **6***

This clause provides a description of the cyber security framework for the ESA-related elements of the DSR system.

A technical solution based on PKI and encryption has been proposed, as it follows well-established industry practice and uses widely implemented technologies, while delivering the policy principles of interoperability, cyber security, grid stability and data privacy.

The security requirements here are proposed because aggregated ESAs connected to the electricity network present a critical national infrastructure risk. Therefore, requirements should go beyond IoT security, while being proportionate to risks and respecting compromises between cost – usability – security.

The security requirements are proposed to protect against the following key high-level risks:

- *CEM/ESA switch load without legitimate request.*
- *CEM/ESA switch load based on incorrect request.*
- *DSRSP tries to switch load of non-legitimate CEM/ESA.*
- *DSRSP tries to switch load based on incorrect information.*
- *Upward (ESA to DSRSP) messages are manipulated or faked.*
- *Downward (DSRSP to ESA) messages are manipulated or faked.*

6.1 Overview

System developers shall ensure that a high degree of cyber security is achieved between the CEM and ESA, at least as secure as in the illustrative examples below.

NOTE At all times, the CA, DSRSP, CEM provider and ESA manufacturer should demonstrate that they are taking all reasonable measures and are following auditable internal security processes in order to ensure that sensitive and confidential information is not accessed by unauthorized parties, i.e. by implementing IEC 2700x.

The following high-level physical-layer-independent cyber security requirements shall be met:

- manufacturers and developers shall conduct a risk assessment and ensure products are appropriately secure and updated to meet the security requirements listed in and referenced by this PAS;
- the CEM and ESA shall be able to obtain and store cryptographic keys and encrypt and authenticate communications to each other;
- the CEM and ESA shall communicate using protocols which contain cyber security protections, e.g. TLS, OCPP or equivalent.

The security measures described in this PAS are put in place in order to mitigate against the following risks:

1. CEM/ESA switch load without legitimate request;
2. CEM/ESA switch load based on incorrect request;
3. DSRSP tries to switch load of non-legitimate CEM/ESA;
4. DSRSP tries to switch load based on incorrect information;
5. upward (ESA to DSRSP) messages are manipulated or faked;
6. downward (DSRSP to ESA) messages are manipulated or faked, i.e.;
   a) threat actor acts as DSRSP to fake flex request to CEM/ESA;
   b) threat actor acts as ESA/CEM to fake flex information to DSRSP;
   c) threat actor intercepts messages to manipulate flex information/requests; and
   d) CEM/ESA firmware/software is manipulated.

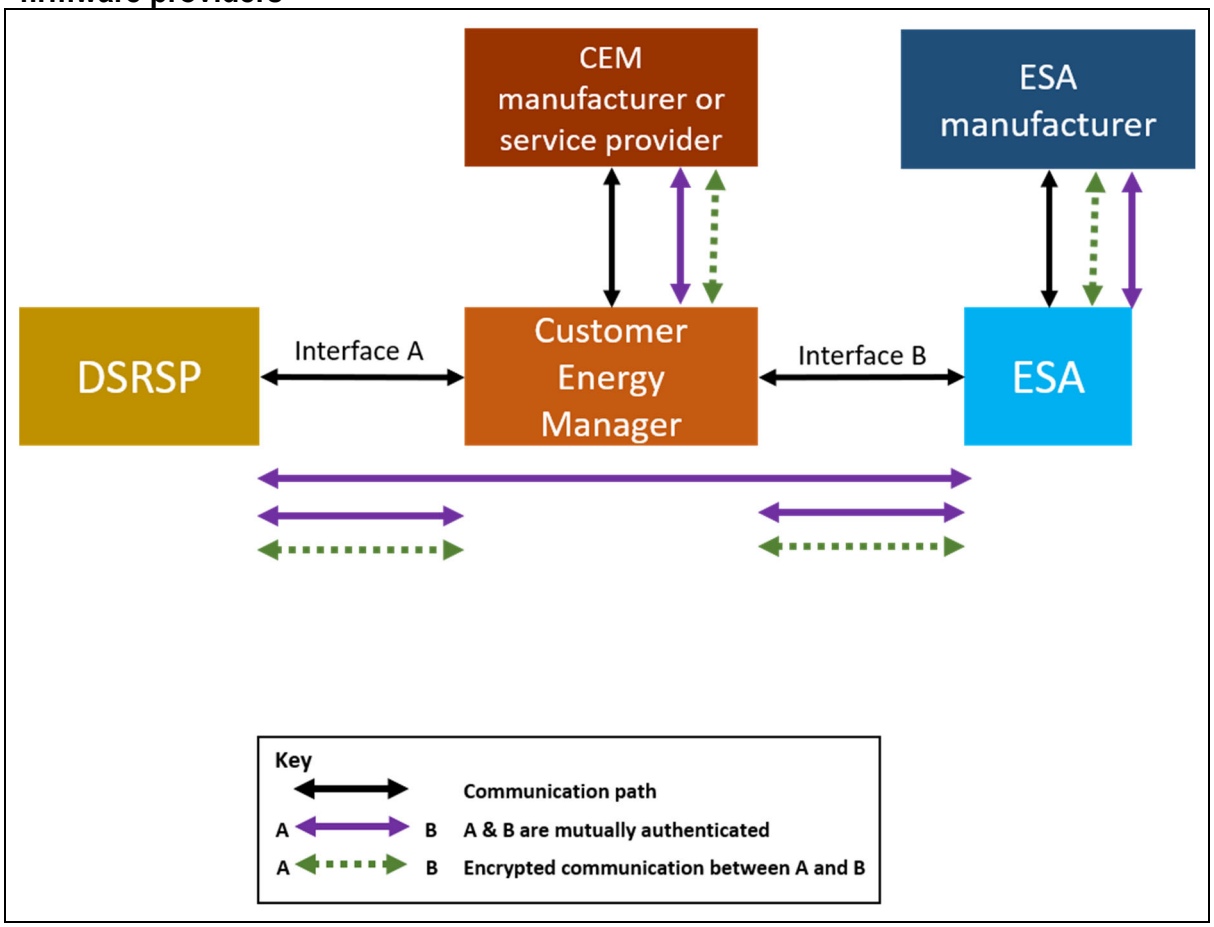
6.2 Cyber security architecture

*COMMENTARY ON **6.2***

The relationship between the DSR architecture components and the CEM and ESA firmware providers is shown in Figure 11. The specific cyber security considerations related to when requests are sent over the GB smart meter network are shown in Annex D.

Throughout this clause, unless otherwise stated, description of communication refers to the network layer and above together with the use of secure application layer protocols such as secure hypertext transfer protocol (HTTPS) and secure WebSocket (WSS), both of which make use of Transport Layer Security (TLS). Public key infrastructure (PKI) is used throughout the system.

Figure 11 – Relationship between DSR architecture components and CEM, ESA firmware providers



Trust authentication operations shall conform to the following.

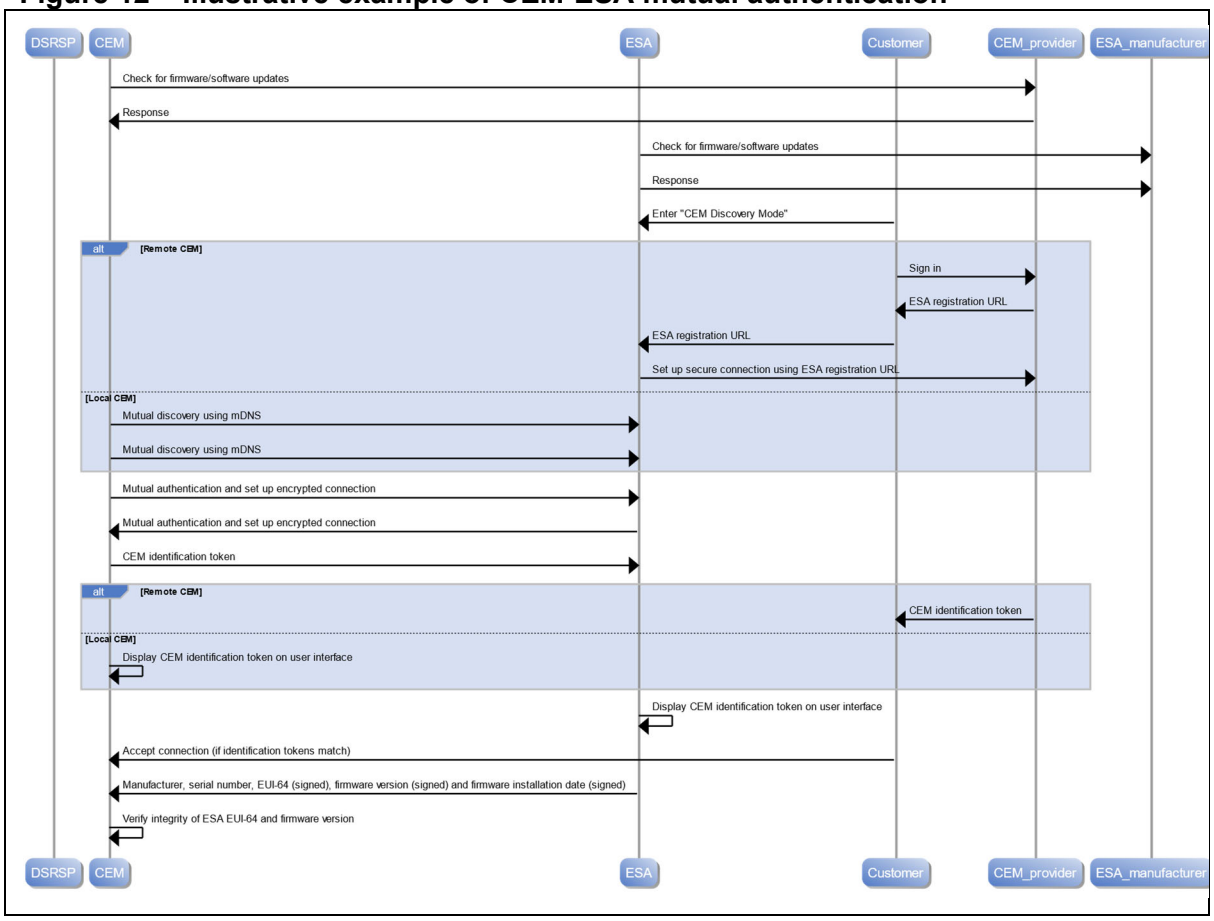
- The ESA shall connect to an external site managed by its manufacturer or provider.
- The ESA and the manufacturer or provider external site shall mutually authenticate and set up an encrypted communications link.
- The CEM shall connect to an external site managed by its manufacturer or provider.
- The CEM and the manufacturer or provider external site shall mutually authenticate and set up an encrypted communications link.
- The CEM and ESA shall mutually authenticate and set up an encrypted communications link.
- The CEM shall be able to mutually authenticate with the DSRSP and set up an encrypted communications link.

- The ESA shall be able to mutually authenticate with the DSRSP.

NOTE 1 Figure 12 shows the components, message flows and scope of trust authentication operations described below.

NOTE 2 In the case that a CEM is located in the cloud and hosted by its manufacturer or service provider, then a communications link between the two might not be required

Figure 12 – Illustrative example of CEM-ESA mutual authentication



Within the context of this PAS, the links between the CEM and ESA and their respective manufacturers or service providers shall be used for non-DSR related commissioning, security credential management (e.g. certificate update) and secure firmware updates.

Within the context of cybersecurity, Interface A shall be used to exchange information required for authentication and certificate management, and transfer signed and encrypted flexibility requests and information between the DSRSP and CEM. The CEM shall also use Interface A to notify the DSRSP of any attempt to compromise operation or stored data of itself or the ESA

The CEM and ESA shall store security sensitive information in a secure, tamperproof, logically separate area.

The CEM and ESA shall incorporate a Security Log in this tamperproof area. The Security Log shall consist of UTC date and time stamped entries of security related information (including tamper and unauthorize access attempt alerts) and may be arranged as a circular buffer. Any passwords used to authenticate the Customer to the ESA, CEM or DSRSP (including web portals and applications) shall either be provided by the manufacturer/service provider or shall be provided by the Customer during initialization or registration. If the password is provided by the manufacturer/service provider then it shall be unique and random and it shall not be based upon easily identifiable publicly available information (e.g.

MAC address). If the password is defined by the Customer then the password shall only be accepted providing that it conforms to certain rules e.g. length, uses symbols and alphanumeric characters and does not use incremental counters (“password1”,”password2” etc.).

6.3 General cyber security

The ESA and CEM shall conform to ETSI TS 303 645.

To be populated with additional existing standards

6.4 Certificate management

The CEM and ESA shall be provisioned by the manufacturer or service provider with updated certificates before the expiry of their existing certificates.

Certificate provisioning shall be carried out using authentication, encryption and signing. The exact process for certificate provision shall be determined by the manufacturer or service provider.

6.5 Secure boot

The ESA and CEM shall operate secure boot processes, such as recommended in the IoT Security Foundation’s Secure Design Best Practice Guides [14].

6.6 Firmware updates

Remote firmware updates shall be securely applied to every ESA and CEM when required by authorized and authenticated entities. This process shall be managed and defined by the manufacturer, who shall be responsible for any third party undertaking the process, and shall maintain the highest cyber security standards. These requirements shall be met for both the update process itself and the management of updates within the manufacturers’, and partners’, organization.

The firmware updates shall be signed and the signature shall be sent to the CEM or ESA for authentication in addition to the firmware image itself.

Appropriate standards to be referenced here

6.7 Security incident management

6.7.1 General

Whenever it is detected that any of the components in the DSR architecture (from DSRSP via CEM to ESA) have been compromised, all other components, actors and systems shall be notified in a manner proportionate to the incident.

6.7.1.1 Event logging and reporting

- The ESA and CEM shall keep a secure record of error/abnormal events or requests.
- ESA or CEM shall report error/abnormal events or requests to DSRSP.

NOTE The DSRSP should keep a secure record of error/abnormal events or requests received from the CEM and ESA and should.report error/abnormal events or information to the independent entity.

6.7.1.2 Vulnerability disclosure

- ESA/CEM manufacturers shall disclose vulnerabilities to secure industry forums.

6.7.2 Attempted unauthorized access

The ESA and CEM shall detect any attempt by unauthorized parties to compromise their operation or access sensitive information by any physical or logical means.

Upon detection of such an attempt on itself, the ESA shall inform the customer and the CEM. The ESA shall generate an entry in its Security Log. The CEM shall inform the DSRSP.

Upon detection of such an attempt on itself, the CEM shall inform the customer, ESA and DSRSP. The CEM shall generate an entry in its Security Log.

6.7.3 Anomaly detection

*COMMENTARY ON **6.7.3***

In addition to the requirements below, the DSRSP and an anomaly detection entity could participate in anomaly detection.

DSRSP detection methods could include analysis of the operation of each component and the analysis of message flows and ESA performance (i.e. anomaly detection).

an anomaly detection entity could be responsible for cross-checking that DSRSP requests to ESAs are congruent with the DSR services requested by grid-side actors. If the anomaly detection entity determines that a request sent is incongruent, then it shall immediately notify the DSRSP and the grid-side actor involved in the request so that corrective action can be taken.

Anomaly detection and response/action, based on:

a) number(or rate) of messages sent/received

b) type of messages sent/received

c) content of message sent/received

This could be based on a defined catalogue of commands, i.e. the Interface A specification, and defined limits of attributes, i.e. agreed at registration.

Checks would be made against privately pre-agreed accepted attributes, values or ranges.

Checks could be made by the DSRSP, the CEM, the ESA (self-checking) or an independent entity (for SMIP this is DCC).

If an independent entity is used message encryption should be considered and messages would need to be sent to/via them also.

Alerts could be issues when thresholds are near.

Actions could be prohibited when thresholds are breached.

The ESA/CEM would only be able to send information within its defined operating capability/limits.

The ESA/CEM would only be able to act on DSRSP messages where the content matches the ESA/CEM sent message and is within its defined operating capability/limits.

The ESA/CEM could only be able to act on or send a fixed number of messages per minute/hour/day (could be thresholds for each, breaching one causes ESA to notify DSRSP and not do as requested) (e.g. to avoid DoS attacks).

The DSRSP would only be able to send a number of messages equivalent to the number of paired CEM/ESAs.

The DSRSP would only be able to send messages where the content matches the received ESA/CEM message or CEM/ESA attributes.

Feedback from public consultation welcome

6.8 Phases of operation

*COMMENTARY ON **6.8***

This clause describes the main phases of the CEM and ESA lifecycle within the context of cyber security:

- *Pre-requisites*
- *Authentication and registration*
- *Normal operation*

- *De-registration*

6.8.1 Pre-requisites

6.8.1.1 Certification authorities

In order for a DSRSP, CEM and ESA to be able to authenticate each other, the DSRSP, CEM and ESA shall be provided with the names (identification) and public keys for all approved certification authorities (CA) in a secure manner.

NOTE 1 A single registration authority exists to grant approval to DSRSPs and CAs (for a specific geography), allowing DSRSPs and CAs to operate as trusted entities in the DSR architecture. Further guidance on registration and certification authorities is provided in PAS 1879.

If an intermediate certification authority is being used to generate certificates, then the CEM and ESA shall be provided with the name and public key of the relevant root certification authority.

NOTE 2 The details of certificate request approval, certificate renewal, provisioning mechanisms and audit requirements are beyond the scope of this PAS.

NOTE 3 Provision of Certification Authority information is performed according to manufacturer specific methods and processes.

6.8.1.2 Network connectivity

The following items in this sub-clause shall be performed according to the methods and processes implemented by the respective manufacturer or service provider.

- The ESA shall be connected to either the customer home network or to a remote communications bearer such as a mobile data connection.
- The local CEM, if present, shall be connected to the customer home network or to a remote communications bearer such as a mobile data connection.
- The local CEM and ESA, if connected to the customer home network, shall be connected to their respective manufacturer or service provider portals via either the home network router or gateway.
- The local CEM and ESA shall be registered with their respective manufacturer or service provider portals.
- Any firmware or security credential updates shall be performed securely, using industry standard processes.

NOTE The CEM and ESA may optionally connect to a smart metering system network. Requirements for connectivity to the GB smart metering system are described in ***Annex D.***

6.8.2 Authentication and registration phase

COMMENTARY ON ***6.8.2***

The authentication and registration phase covers the period from when the user of the ESA initiates the DSRSP subscription process to the time at which DSR service messages are able to be transferred.

This phase is divided into the following sub-phases:

- *DSRSP service customer registration;*
- *CEM and ESA mutual authentication; and*
- *DSRSP and CEM authentication and registration.*

6.8.2.1 DSRSP service customer registration

The customer shall be provided with certain information by the CEM service provider that is to be used during the CEM/ESA DSRSP service authentication and registration processes.

The customer shall be provided with at least the following information:

- CEM service provider name;

- CEM manufacturer name; and
- CEM serial number.

The customer shall begin the registration process for the DSRSP service using a medium other than the CEM or ESA (e.g. internet portal, phone, mail or in person).

The DSRSP shall be provided with at least the following information:

- CEM service provider name;
- CEM manufacturer name;
- CEM serial number;
- Customer Electricity Supplier; and
- Agreement to contract DSR services.

The customer shall be provided with at least the following information by the DSRSP that is to be used during the CEM and ESA DSRSP service authentication and registration processes:

- CEM registration URL; and
- DSRSP identification token.

NOTE The details of the DSR service registration process are determined by the DSRSP and are beyond the scope of this PAS. For example, the DSRSP may contract an Agent to act on their behalf to complete some elements, in this situation the DSRSP remains responsible for compliance with this PAS, both for themselves and for any Agents acting on their behalf.

6.8.2.2 CEM and ESA mutual authentication

*COMMENTARY ON **6.8.2.2***

Interface B, between the ESA and CEM, is defined by the ESA manufacturer and/or the CEM provider and is not considered in detail in this PAS. Therefore this PAS describes general requirements for the CEM/ESA discovery, authentication and enduring communications processes.

Mutual authentication and the establishment of secure communications between the CEM and ESA shall meet the following requirements.

a) The latest CEM and ESA firmware and/or software versions with no known cyber security vulnerabilities shall be successfully installed prior to commencement of the authorization process.

b) The process shall result in unambiguous, secure mutual authentication of the CEM and ESA.

c) The process shall result in a secure connection between the CEM and ESA.

d) Industry best practice and standards shall be used throughout the authentication process.

e) The process shall minimize involvement of the Customer.

f) Public Key Infrastructure methods shall be used.

g) Certificates shall be provided by an approved Certification Authority.

h) An encrypted link shall be set up between the CEM and ESA following successful certificate based authentication, using the latest version of TLS.

i) Additional unambiguous identification methods shall be used as a second stage of authentication and shall make use of either the encrypted link or other secure communication paths (e.g. “identification number” sent to Customer via SMS for entry into CEM or ESA).

j) Any token input used as part of the process shall be subject to a limited time window and shall indicate such to the Customer (e.g. countdown timer displayed for input of “identification number”).

k) Any errors encountered during the process shall be notified to the Customer and the manufacturer or service provider.

l) The ESA shall pass information on its manufacturer, model, EUI-64, firmware version and firmware installation date to the CEM over a secure link.

m) The CEM may perform validation of the information provided by the ESA using a 3rd party.

6.8.2.2.1 Illustrative example of CEM-ESA mutual authentication process

NOTE 1 This process is also depicted in Figure 12.

NOTE 2 The ESA and CEM may be pre-provisioned with the information required for mutual authorization, for instance if they are provided by the manufacturer as a pair.

a) The CEM shall check for firmware/software updates with no known cyber-security vulnerabilities and perform a secure update if a more recent version is available.

b) The ESA shall check for firmware/software updates with no known cyber-security vulnerabilities and perform a secure update if a more recent version is available.

c) The ESA shall be placed into “CEM discovery mode” by the Customer (DSRSP subscriber).

d) If a remote CEM is used:

- Customer shall sign in to the CEM service portal;
- the CEM service provider shall provide the Customer with an ESA registration URL using the CEM service provider portal;
- the ESA shall be provided with the ESA registration URL by the customer; and
- the ESA shall contact the ESA registration URL over a secure connection using the latest version of TLS.

e) If a local CEM is used ,the CEM and ESA shall discover each other using mDNS.

f) The CEM and the ESA shall mutually authenticate using their respective certificates.

g) An encrypted link shall be set up between the CEM and ESA using the symmetric key produced as part of the TLS handshake.

h) The CEM shall send a CEM identification token to the ESA:

a. if a remote CEM is used, the CEM service provider shall send the token to the Customer via the CEM service provider portal;

b. if a local CEM is used, the local CEM shall display the token on its user interface.

i) The ESA shall display the token on its user interface.

j) If the ESA displayed token matches the token provided to the customer, the customer shall accept the CEM and allow connection to be set up.

k) The ESA shall send its manufacturer name, serial number, EUI-64, firmware version and firmware installation date to the CEM over a secure link. The EUI-64, firmware version and firmware installation date shall be signed by the ESA manufacturer.

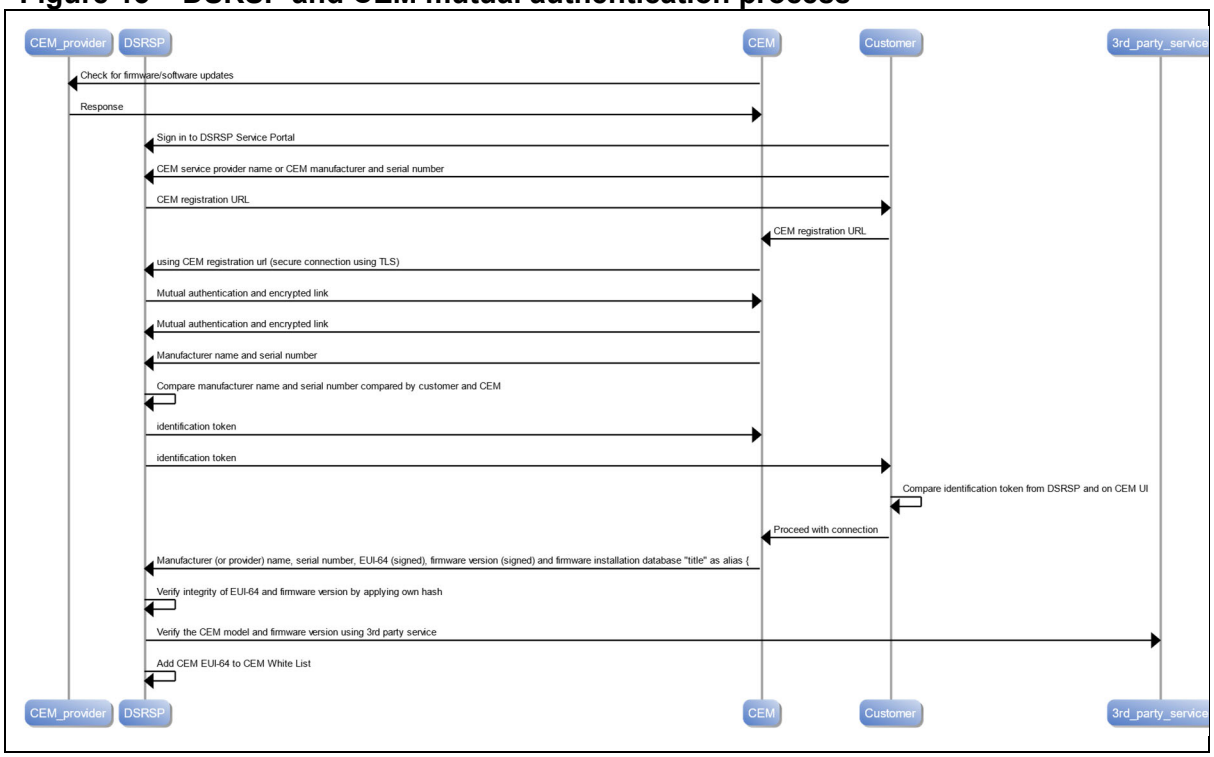
l) The CEM shall verify the integrity of the ESA EUI-64 and firmware version by comparing the manufacturer signature hash with that of its own.

NOTE 3 The CEM can verify the ESA model and firmware version using a 3rd party connection.

6.8.2.3 DSRSP and CEM

The DSRSP and CEM shall mutually authenticate using the following process, as depicted in Figure 13:

Figure 13 – DSRSP and CEM mutual authentication process



a) The CEM shall check for firmware/software updates with no known cyber-security vulnerabilities and perform a secure update if a more recent version is available.

b) Customer shall be able to sign in to the DSRSP service portal, agree to contract DSR services and request “register a CEM”.

NOTE 1 The details of this process are determined by the DSRSP and are beyond the scope of this PAS.

c) Customer shall be able to provide the DSRSP with CEM information including CEM service provider name , manufacturer name and serial number (any additional required information shall be determined by the DSRSP).

d) The DSRSP shall be able to provide the Customer with a CEM registration URL and password.

e) The Customer shall be able to enter the CEM registration URL using the CEM user interface.

NOTE 2 The CEM user interface may include a web page , App or built-in user interface.

f) The CEM shall contact the CEM registration URL over a secure connection using the latest version of TLS.

g) The CEM shall be able to mutually authenticate with the DSRSP using their respective certificates.

h) An encrypted link shall be set up between the CEM and DSRSP using the symmetric key produced as part of the TLS handshake.

i) The CEM shall send its manufacturer name and serial number to the DSRSP over the encrypted link.

j) The DSRSP shall be able to check that the manufacturer name and serial number sent by the CEM matches that provided by the Customer.

   1) If the information does not match then the Customer shall be informed and no further action needs to be be taken by the DSRSP.

k) The CEM shall be able to receive a DSRSP identification token from the DSRSP and shall display this token on its user interface (the DSRSP should send the same identification token to the Customer).

l) If the two tokens match then the Customer shall be able to accept the DSRSP and allow the connection with the CEM to proceed (otherwise the user can inform the DSRSP and the registration process can be terminated by the DSRSP).

m) The CEM shall send its manufacturer, serial number, EUI-64, firmware version and firmware installation date to the DSRSP over a secure link. The EUI-64 and firmware version shall be signed by the ESA manufacturer.

n) The DSRSP shall be able to verify the integrity of the CEM EUI-64 and firmware version by comparing the manufacturer signature hash with that of its own.

o) The DSRSP shall be able to verify the CEM model and firmware version using a 3rd party service connection.

p) If the CEM verification is successful then the DSRSP shall be able to add the CEM EUI-64 to its CEM Allowed List.

q) If already obtained through the CEM and ESA mutual authentication process, the CEM shall send the ESA manufacturer name, serial number, EUI-64, firmware version and firmware installation date to the DSRSP over a secure link. The EUI-64 and firmware version shall be signed by the ESA manufacturer.

r) The DSRSP shall be able to verify the ESA model and firmware version using a 3rd party connection.

s) If the ESA verification is successful then the DSRSP shall be able to add the ESA EUI-64 to its ESA White List.

t) The CEM shall then enter normal operation with the DSRSP.

6.8.3 Operation phase

In normal operation, messages shall be sent over Interface A between the DSRSP and CEM and over Interface B between the CEM and ESA. The CEM and ESA shall decrypt, authenticate, encrypt and sign messages, as appropriate, sent between the CEM and ESA/DSRSP.

The ESA and CEM shall only accept and act on messages from their paired DSRSP/CEM/ESA, authenticated through the use of signatures in every message.

The ESA and CEM shall only send DSR related messages to their paired DSRSP/ESA/CEM, including their signature in every message for authentication.

NOTE All messages in the operation phase are required to be encrypted as they are load affecting (either directly e.g. flexibility requests or indirectly e.g. flexibility updates) and hence pose a risk to grid stability. All messages in the authentication and registration phase are required to be encrypted to ensure data privacy and cyber security.

6.8.3.1 Interface A messages

Messages sent over Interface A shall conform to the security requirements in the specified interface protocol in Clause **5**.

Messages sent from the CEM to the DSRSP shall include:

a) ESA and CEM information used during the authentication and registration phases, which shall be encrypted and signed by the CEM;

b) ESA flexibility offers and forecast updates, which shall be encrypted and signed by the CEM;

c) ESA status information, which shall be encrypted and signed by the CEM;

d) certificate update notification and new certificates, which shall be signed by the CEM;

e) ESA or CEM originated de-registration notification, which shall be encrypted and signed by the CEM; and

f) notification of tampering or attempted tampering of the CEM or ESA, which shall be encrypted and signed by the CEM.

Messages that the CEM shall be able to receive and act on from the DSRSP include:

1) information sent by the DSRSP during the CEM and ESA authentication and registration processes, which shall be encrypted and signed by the DSRSP;

2) requests for ESA status updates, which encrypted and signed by the DSRSP;

3) ESA flexibility offer selection messages, encrypted and signed by the DSRSP;

4) DSRSP originated CEM or ESA de-registration notification, encrypted and signed by the DSRSP; and

5) certificate update notification and new certificates, signed by the DSRSP.

6.8.3.2 Interface B messages

Messages sent over Interface B shall conform to any security requirements in the implemented interface protocol

Messages sent between the ESA and CEM shall include:

a) ESA information used during the mutual authentication phase, which shall be encrypted and signed by the ESA;

b) ESA flexibility offers and forecast updates, which shall be encrypted and signed by the ESA;

c) ESA status information, which shall be encrypted and signed by the ESA;

d) certificate update notification and new certificates, which shall be signed by the CEM;

e) ESA originated de-registration notification, which shall be encrypted and signed by the ESA; and

f) notification of tampering or attempted tampering of the ESA, which shall be encrypted and signed by the ESA.

g) Error and fault notification messages, which shall be encrypted and signed by the ESA

Messages sent between the CEM and ESA shall include:

1) information sent by the CEM during the CEM and ESA phase, which shall be encrypted and signed by the CEM.

2) requests for ESA status updates from the DSRSP, which shall be encrypted and signed by the CEM.

3) ESA flexibility offer selection messages from the DSRSP, which shall be encrypted and signed by the CEM.

4) certificate update notification and new certificates, which shall be signed by the CEM;

5) CEM originated ESA de-registration notification, which shall be encrypted and signed by the CEM; and

6) notification of tampering or attempted tampering of the CEM, which shall be encrypted and signed by the CEM.

7) Error and fault notification messages, which shall be encrypted and signed by the CEM

6.8.4 De-registration

COMMENTARY ON 68.4

The de-registration of a CEM or ESA from a DSRSP service can be instigated either by the customer or by the DSRSP.

De-registration of a CEM or ESA shall disassociate it from a DSRSP service. A de-registered CEM or ESA shall securely delete (remove) any information stored on it that is associated with the DSRSP service and shall request the DSRSP to delete (remove) any information stored that is associated with the CEM, ESA or customer. A de-registered CEM or ESA shall be able to re-join the DSRSP service only through the registration process described in **6.8.2.1** and **6.8.2.2**.

A customer shall request that a CEM or ESA is de-registered by first contacting the DSRSP. The subsequent process is determined by the DSRSP and shall involve encrypted, signed messages and customer interaction.

NOTE A DSRSP should inform the customer that a CEM or ESA is being de-registered before the de-registration process is initiated.

7 General requirements of an ESA

*COMMENTARY ON CLAUSE **7***

These requirements relate only to energy flexibility related aspects of the ESA. Other aspects, for example remote diagnostics and maintenance, remote programming etc., are not within the scope of this PAS.

7.1 General

An ESA shall conform to all standards applicable to the equivalent non-energy-smart appliance.

Each ESA shall be supplied with a CEM.

An ESA should not be prevented from connecting to a different CEM to the one with which it was originally supplied.

The ESA shall be able to provide as a minimum an “intended operation” (IO) power profile, a “least delayed” (LD) power profile and a “most delayed” (MD) power profile when required (see **5.5.4**).

When reporting forecast power profiles, the ESA shall take into account its operating capabilities, consumer preferences (when available) and external information (when available) as necessary.

The CEM shall operate according to the four operating modes specified in **5.3.5.1**.

The CEM shall use the operating mode priority ordering specified in **5.3.5.2**.

7.2 ESA architecture

An ESA shall exchange information with any authorized DSRSP via the ESAG and CEM or smart metering system.

NOTE 1 The physical layer is not specified.

An ESAG shall connect to a CEM.

A CEM shall connect to no more than one DSRSP at any given time.

An ESA shall be connected to no more than one CEM and one DSRSP at any given time.

An ESA shall include a manufacturer-defined Interface B as shown in Figure 4.

The CEM shall be able to translate between the Interface A and Interface B data models without the loss of any information.

The flexibility information and requests passed over the interface between the CEM and DSRSP (Interface A) shall conform to those described in **5.3** and **5.4**.

If an ESA interfaces to the GB smart metering system, it shall do so according to Annex D.

An ESA shall contain a means of reporting its own individual power consumption or production, rather than that of the premises, by monitoring and recording its power values, either through a state machine lookup table or direct measurement.

NOTE 2 In countries where the ESA can connect to a smart meter system, the ESA can receive smart metering information over the Interface B.

NOTE 3 The ESA can incorporate one or more additional interfaces, denoted the “manufacturer interface” in Figure 4. Such interfaces are out of the scope of this PAS, although example uses include remote maintenance and remote selection of programmes by the consumer.

7.3 Consumer action

If supplied together, either the ESA or the CEM shall provide a user interface that enables the consumer to provide their preferences for ESA operation and DSR service provision and gives the consumer the ability to manually override, in real-time, current and planned DSR operations.

If the ESA and CEM are supplied separately, the ESA shall provide a user interface that enables the consumer to provide their preferences for ESA operation and DSR service provision and gives the consumer the ability to manually override, in real-time, current and planned DSR operations.

If supplied together, either the ESA or the CEM shall provide a user interface that provides the consumer with DSR-related information including, but not limited to, current DSR status, planned DSR operation , and power consumption.

If the ESA and CEM are supplied separately, the ESA shall provide a user interface that provides the consumer with DSR-related information including, but not limited to, current DSR status, planned DSR operation, and power consumption.

The ESA and/or CEM shall inform the consumer of any planned or current ESA/DSR flexibility operation if configured to do so according to customer preferences.

NOTE The ESA and/or ESAG and/or CEM may provide the consumer with cost saving information relating to the energy performance of the ESAs on a regular or ongoing basis.

The ESA and/or CEM shall be capable of providing the consumer (if necessary through a connected device) with an accessible communications interface (e.g. adjustable text sizes, voice read-out, large buttons). Options chosen shall be preserved when software is updated.

The ESA shall provide the consumer with the means to enable and disable its “energy smart” functionality.

7.4 Installation and initiation

An ESA shall not be contracted to (or controlled by) more than one DSRSP at any one time, although DSRSPs may pool ESA control capacity into aggregated control loads for different purposes.

Installation of the energy smart functionality of an ESA, ESAG and CEM shall be possible without the intervention of a third party (i.e. installer), unless such intervention is required by local regulation (e.g. for a smart EV chargepoint).

The ESA shall conform to all applicable installation guidelines and standards applicable in the country of sale.

Upon power-up, the ESA smart interface shall begin a secure network discovery and connection process (applies to communications network connection).

Unless the ESAG and CEM are incorporated in the ESA, upon secure network connection, the ESA and ESAG shall mutually identify and authenticate themselves. If the ESAG and CEM are separate entities, the ESAG and CEM shall mutually identify and authenticate themselves.

The CEM and DSRSP shall also mutually identify and authenticate themselves, and the ESA and DSRSP shall mutually authenticate their communication.

Following authentication, the ESA shall exchange information with the DSRSP, via the ESAG and CEM, concerning its flexibility capabilities.

*NOTE Installation use cases are described in Annex A, **A.1**.*

7.5 General operation

The general operation of the ESA and CEM shall conform to that of the modes described in Table 1.

7.6 Safety

The ESA shall be configured such that safety aspects take priority over energy flexibility related behaviour at all times.

7.7 Power value or profile provision

The provision of power values or profiles shall conform to that described in **5.6**.

7.8 Fault conditions

In the event of a loss of communications between the ESA and the DSRSP, the ESA shall continue with its currently selected flexibility option and log its power consumption periodically for transmission to the DSRSP whenever communications are resumed.

NOTE 1 If deemed necessary by the DSRSP, the DSRSP can include a timeout value in the flexibility offer request message to a CEM or ESA, upon the expiry of which the ESA shall revert to routine mode if it has not already done so.

In the case of exception conditions (e.g. fault, power loss), the ESA shall transition or reset to a mode that brings it into a safe state. The ESA shall report its change in flexibility status to the DSRSP whenever possible.

NOTE 2 The mode to bring the ESA into a safe state depends upon the ESA type and the manufacturer.

When recovering from an unexpected loss of power, the ESA shall regain connectivity and time synchronization with the ESAG and initialize its flexibility status within 10 min.

When recovering from an unexpected loss of power, the ESAG shall regain connectivity and time synchronization with the CEM and transfer its ESA flexibility status to the CEM within 10 min.

7.9 Time

The CEM and ESA shall use a UTC time reference. The CEM and ESA shall synchronize local clocks with an external time reference at least once every 24 hours. In the event of a loss of communication, the ESA shall maintain a local clock aligned with the master clock to within ±10 s per day.

If the flexibility request is actioned by the DSRSP, the ESA shall begin flexibility operations within a time to be specified by the DSRSP (this may vary according to the type of flexibility request).

The ESA shall send a message in order to notify its ESAG, CEM or DSRSP of any change in flexibility capability within 10 s.

The ESA shall apply randomized offsets as described in **5.5.4.5**.

NOTE ToU tariff period start times might be subject to a randomized offset, as determined by the supplier. It is expected that this is implicit to the smart metering service and so is beyond the scope of this PAS 1878.

7.10 Optional frequency-based services

If they have the capability, ESAs shall perform frequency-based services as described in **5.5.5** and **5.5.6**.

7.11 Physical protection

The integrity of ESAs shall be protected by physical means, e.g. ensuring a tamper-protection boundary to deter access to key components.

An ESA shall securely maintain a tamper alert log.

An ESA shall immediately attempt to inform both the customer and the DSRSP if it detects a tamper attempt.

7.12 Privacy

Existing regulations which indicate compliance with data privacy laws shall apply, e.g. only the minimum amount of data needed to operate a DSR service shall be shared with DSRSPs.

NOTE Where possible, tariff information should be obtained directly by the ESA (and not passed to the DSRSP), rather than being obtained via the DSRSP for the ESA. The DSRSP does not need to know the tariff information in most installations in order to provide called DSR services.

Consumers shall be in control of any data arising from ESAs that is exchanged with third parties, with clear consent procedures that enable them to make informed decisions regarding data sharing.

Data shall be securely stored when on the device or with any controlling party, and shall be capable of being securely removed when the device is recycled, reused or disposed of.

Data shall be securely transmitted between devices or any controlling parties, as specified in **7.13**.

7.13 Cyber security

A CEM/ESAG/ESA shall conform to ETSI TS 303 645 and to Clause **6**.

A CEM/ESAG/ESA shall be configured such that only authorized and trusted entities are able to connect to its logical interfaces.

A CEM/ESAG/ESA shall be configured such that any logical interfaces not connected to an authorized and trusted entity are closed (e.g. unused IP ports are closed).

A CEM/ESAG/CEM shall not expose any physical interfaces (e.g. JTAG port) to unauthorized users.

CEM/ESAG/ESA firmware shall be protected, and firmware updates shall be made secure.

Data held by CEM/ESAG/ESAs shall be protected.

Messages sent to CEMs and ESAs shall be sent from a certified and trusted source.

If an ESA, ESAG or CEM implements the optional interface to an external system then the interface shall be at least as secure as the DSRSP/CEM interface (Interface A).

7.14 Lifecycle

This subclause will contain any priority ESA requirements not covered elsewhere in the PAS, related to lifecycle consideration such as software updates and the second-hand market for ESAs.

8 Specific ESA requirements

8.1 Smart EV chargepoint

When reporting flexibility offers to the DSRSP, the smart EV chargepoint shall take into account the battery capacity of the EV as well as the physical operating limits of the EV (in addition to those of the smart EV chargepoint) whenever available.

If a smart EV chargepoint supports V2G functionality and has been configured to present itself to the DSRSP as an ESA, then it shall meet the information and messaging requirements specified in Clause **5**.

NOTE Smart EV chargepoints are not required to support V2G functionality.

8.2 Battery storage

Battery storage systems shall be capable of reporting both charging and discharging “least delayed” (LD) and “most delayed” (MD) forecast power profiles in addition to an “intended operation” (IO) forecast power profile to the DSRSP.

Energy charging profiles shall have positive energy profiles; energy discharging profiles shall have negative energy profiles.

8.3 HVAC appliances

HVAC systems shall be capable of reporting forecast power profiles based on operating capabilities, consumer preferences and external information, to include the consumer’s desired maximum and minimum temperature excursions based on estimates of the heat load and heat storage properties of the buildings.

Annex A (informative)
Use cases

This Annex will be used to describe the use cases used to identify requirements for the PAS and to illustrate operational examples.

External case documents will be referenced as appropriate, once selected.

The use cases listed below are included as examples and will be further developed in subsequent versions

Several ESA and DSR use cases will be aligned in future versions, as key use cases are agreed

There will be scope to amend these use cases and SG comments are welcome.

A.1 Set-up type use cases

A.1.1 ESA is installed and setup (consumer installation, first turn on)

A.1.1.1 Aim

1) ESA is authenticated to DSRSP and to any relevant intermediate components.
2) ESA is able to exchange energy flexibility messages with DSRSP and relevant intermediate components.

A.1.1.2 Assumptions

1) ESA is installed by consumer

A.1.1.3 Pre-conditions

1) ESA is in situ in consumer premises
2) Consumer HAN is operational
3) DSRSP WAN is operational

A.1.1.4 Actors and components

1) DSRSP
2) Consumer
3) ESA
4) CEM

A.1.1.5 Sequence

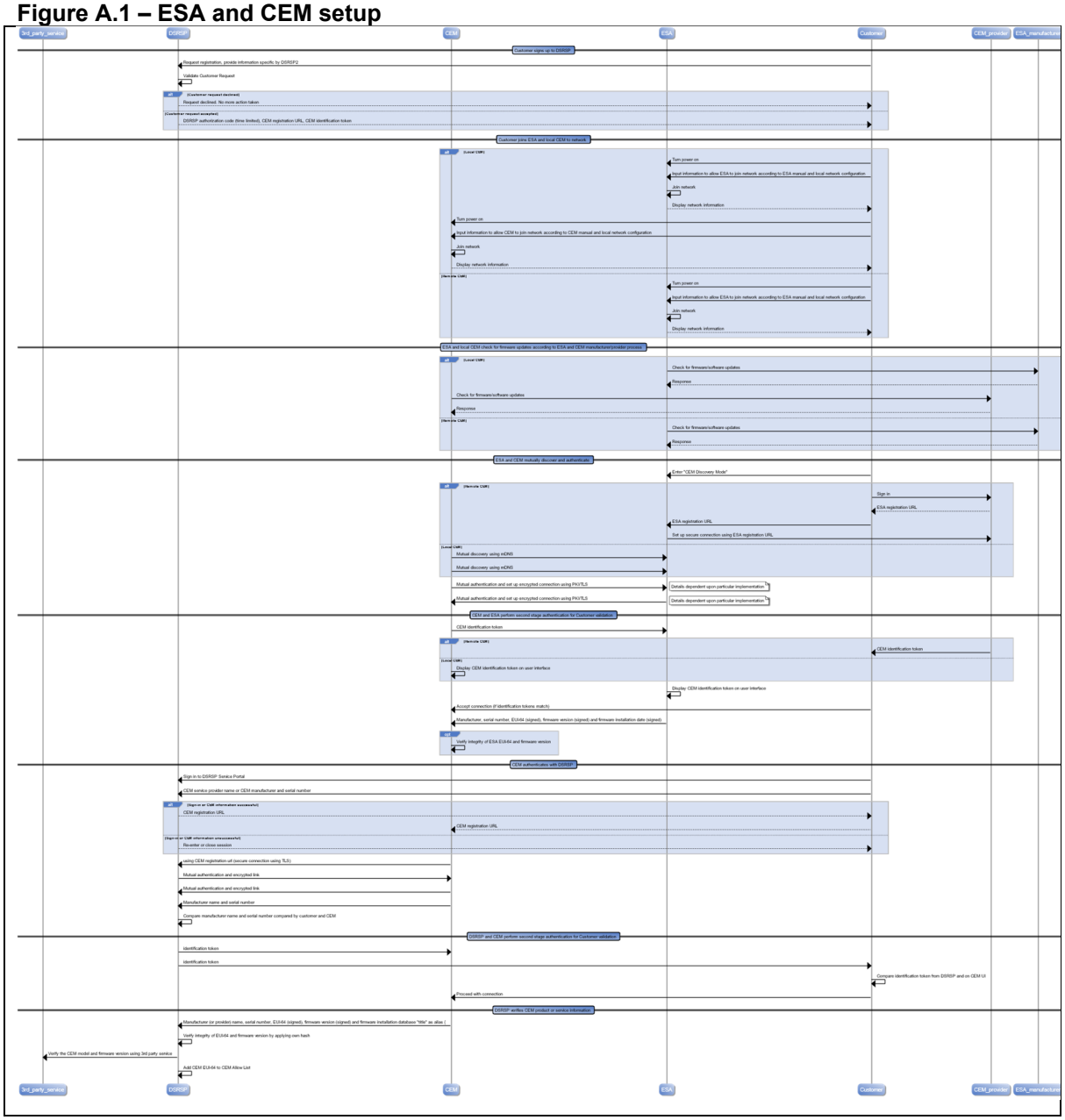
An example sequence of interactions required for ESA and CEM mutual authentication and for ESA/CEM and DSRSP mutual authentication is depicted in Figure A.1 and may be summarized as:

1. Customer registers with DSRSP and receives time limited registration information to provide to the ESA and/or CEM (using a process defined by the DSRSP);
2. Customer joins the ESA and the local CEM to the (local) network (no action is required for a remote CEM);
3. the ESA and local CEM perform firmware updates as required;
4. the ESA and CEM mutually discover and authenticate using best practice methods;
5. the ESA and CEM perform a secondary authentication procedure requiring Customer approval;
6. the CEM adds the ESA to its “ESA Allow list”;
7. Customer signs in to the DSRSP Service Portal and provides information on the CEM. If successful, the DSRSP responds by providing a limited lifetime CEM

registration URL, which the Customer provides to the CEM (using a CEM specific process);

8. the CEM and DSRSP mutually authenticate using best practice methods;
9. the CEM and DSRSP perform a secondary authentication procedure requiring Customer approval; and
10. the DSRSP adds the CEM to its “CEM Allow list”.

Figure A.1 – ESA and CEM setup



A.1.2 ESA is subscribed to a different DSRSP (consumer switching)

A.1.2.1 Aim

The ESA and CEM are successfully de-registered with existing DSRSP and registered with a new DSRSP.

A.1.2.2 Assumptions

The new DSRSP is compliant with Interface A.

A.1.2.3 Pre-conditions

1) The ESA and CEM are installed in premises and subscribed to a DSRSP energy flexibility service.
2) The ESA and CEM have network connectivity.

A.1.2.4 Actors and components

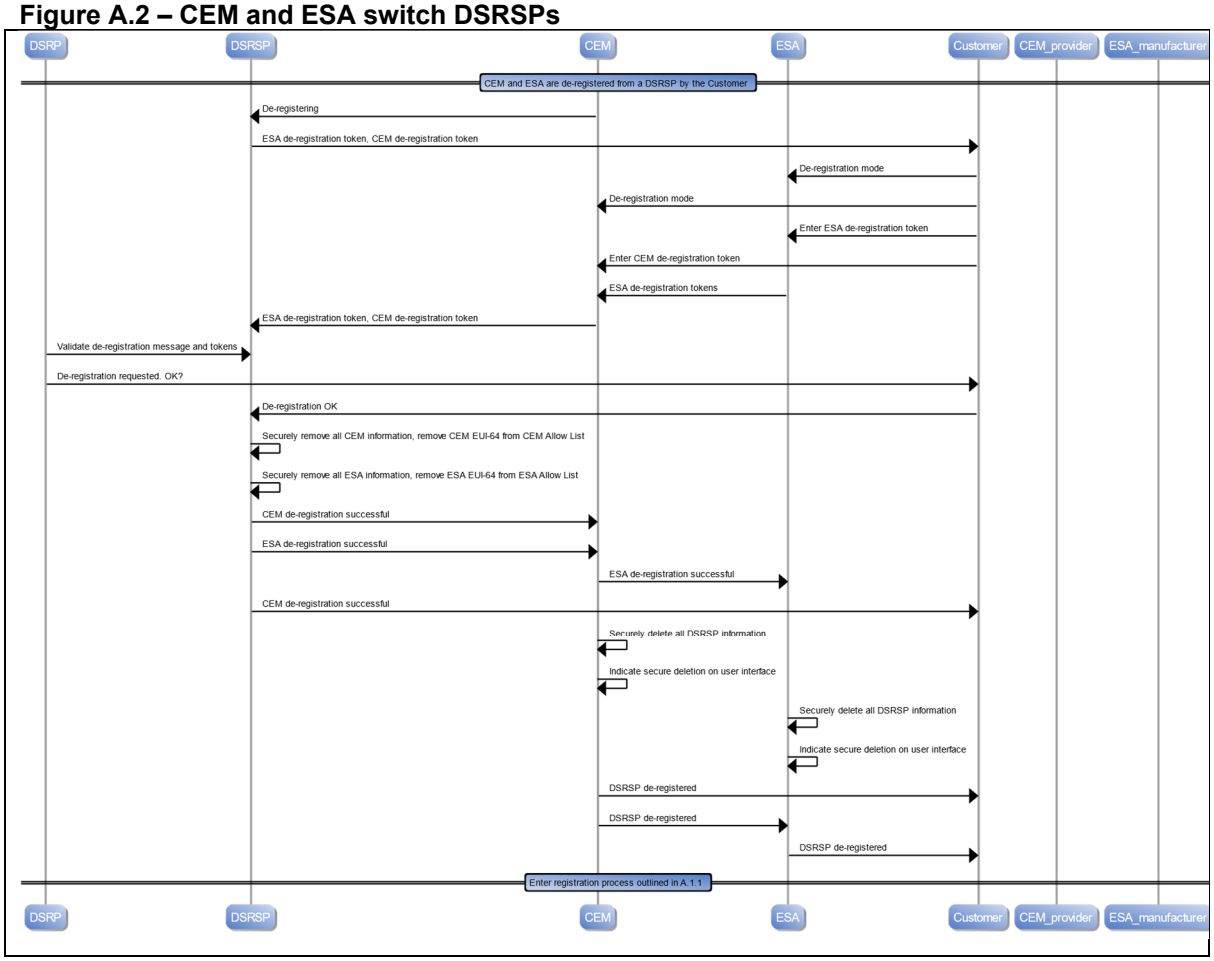
1) DSRSP
2) Consumer
3) ESA
4) CEM

A.1.2.5 Sequence

The details of the de-registration process are determined by the DSRSP. However, the process will require the use of de-registration messages over Interface A and should include certain checks and balances in order to mitigate unauthorized de-registration. An example sequence is listed below and depicted in Figure A.3.

1) Customer contacts the incumbent DSRSP and requests de-registration of an ESA and CEM;
2) Customer is provided with a token each for the ESA and CEM by the DSRSP;
3) Customer enters “de-register DSRSP” mode in both the CEM and DSRSP and enters the respective de-registration tokens;
4) the ESA sends its de-registration token to the CEM;
5) the CEM sends both its own de-registration token and that of the ESA to the incumbent DSRSP in a “de-registration” message;
6) the DSRSP validates the de-registration message and the tokens and contacts Customer for validation of the de-registration;
7) upon customer validation, the DSRSP marks all appropriate information relating to the ESA, CEM and Customer for deletion, removes the CEM from its “CEM Allow list” and sends a “de-registered” response message to the CEM and ESA;
8) the CEM and ESA remove all appropriate DSRSP information from their storage; and
9) the registration process described in A.1.1 is invoked by the Customer to register with a new DSRSP.

Figure A.2 – CEM and ESA switch DSRSPs



A.1.3 ESA is de-registered from a CEM by the Customer

A.1.3.1 Aim

The ESA is successfully de-registered from the CEM. All CEM and DSRSP information is securely removed from the ESA, with all actions logged by the ESA. All ESA information is securely removed from the CEM and DSRSP, with all actions logged.

A.1.3.2 Assumptions

None

A.1.3.3 Pre-conditions

3) The ESA and CEM are installed in premises and subscribed to a DSRSP energy flexibility service.

4) The ESA and CEM have network connectivity.

A.1.3.4 Actors and components

5) DSRSP

6) Consumer

7) ESA

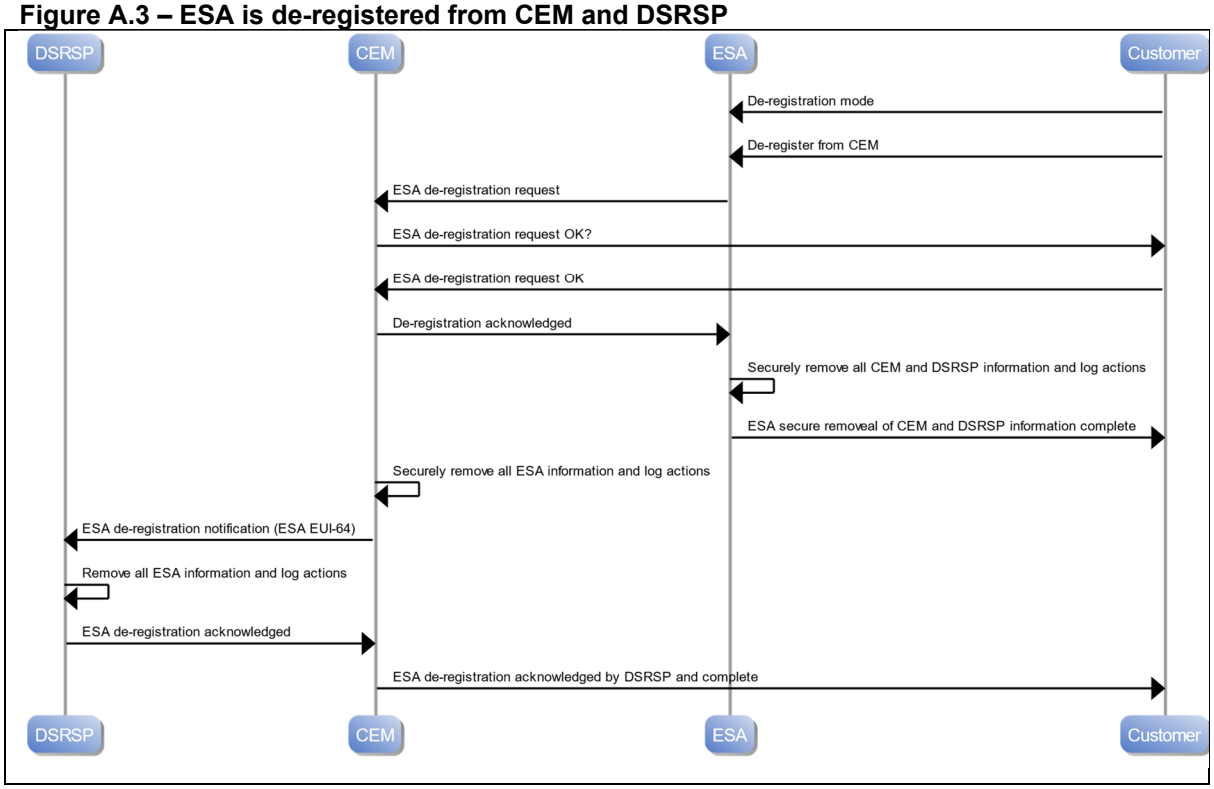
8) CEM

A.1.3.5 Sequence

An example sequence of interactions required for ESA de-registration is depicted in **Error! Reference source not found.** and may be summarized as:

1) Customer places the ESA into de-registration mode;
2) Customer selects “de-register from CEM”;
3) the ESA sends a de-registration request to the CEM;
4) the CEM awaits for confirmation of ESA de-registration from the Customer (via the CEM UI);
5) the Customer confirms the ESA de-registration to the CEM;
6) the CEM sends a “de-registration confirmed” message to the ESA;
7) the ESA securely removes all information related to the CEM and DSRSP, logging all actions;
8) the ESA informs the Customer that it securely removed all CEM and DSRSP information;
9) the CEM securely removes all information related to the CEM and DSRSP, logging all actions;
10) the CEM sends an “ESA de-registration notification” message to the DSRSP;
11) the DSRSP securely removes all information related to the ESA and logs all actions;
12) the DSRSP sends an “ESA de-registration acknowledged” message to the CEM and
13) the CEM informs the Customer that the ESA de-registration process is complete and that ESA information has been removed from the DSRSP.

Figure A.3 – ESA is de-registered from CEM and DSRSP



A.2 Operation type use cases

A.2.1 ESA is powered up (non-first turn on)

This use case will be populated following steering group review.
It could consider the specific case for an EV plugged into a smart EV chargepoint.

A.2.1.1 Aim

The ESA has been authenticated and is ready to receive requests from the DSRSP.

A.2.1.2 Assumptions

The ESA has already been authenticated by the CEM and DSRSP.

A.2.1.3 Pre-conditions

1) The ESA and CEM are installed in premises and subscribed to a DSRSP energy flexibility service.
2) The ESA and CEM have network connectivity.
3) The ESA has already been authenticated by the CEM and DSRSP.

A.2.1.4 Actors and components

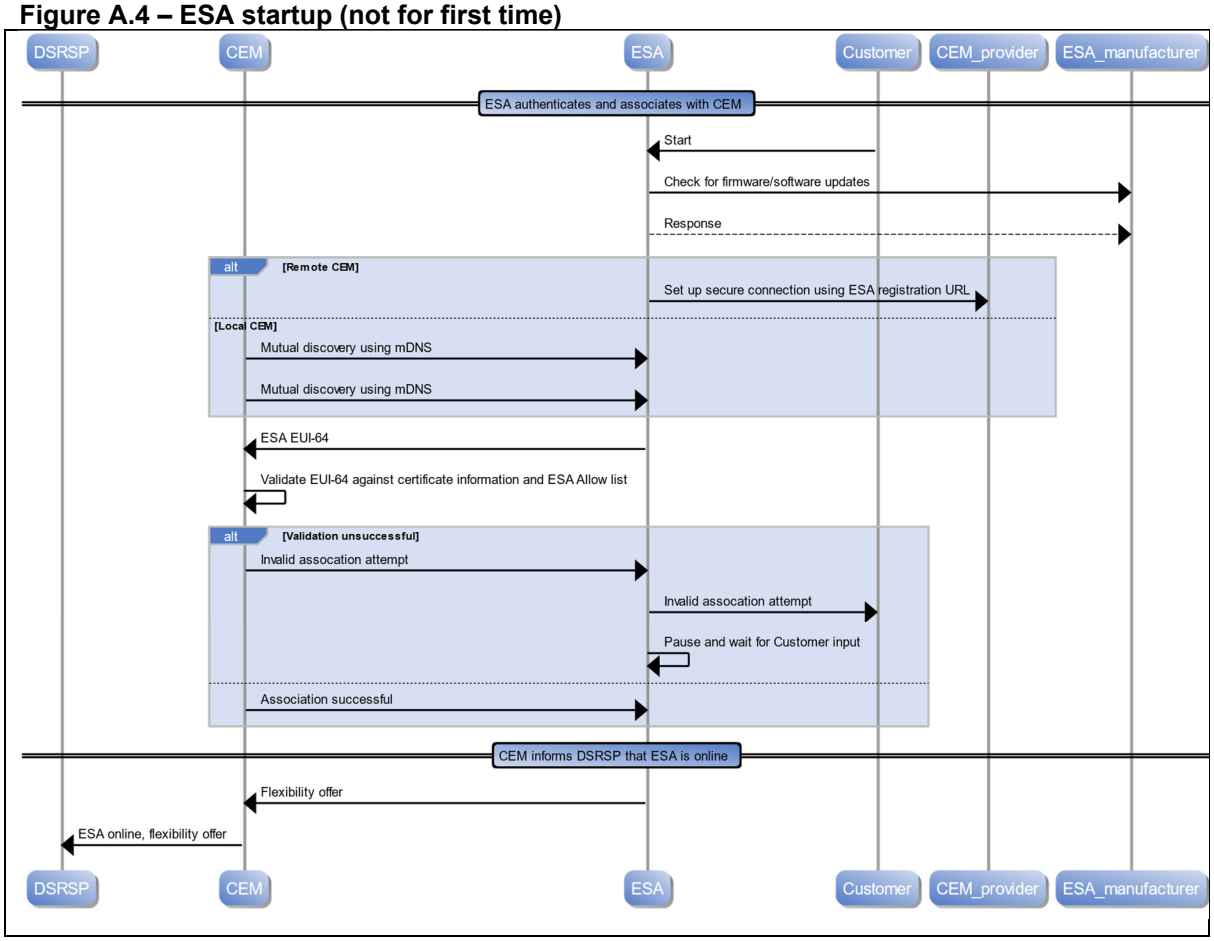
1) DSRSP
2) ESA
3) CEM

A.2.1.5 Sequence

An example sequence is depicted in Figure A.4. The main steps are:

1) Customer starts the ESA;
2) the ESA checks for firmware update;
3) the ESA and CEM mutually identify and authenticate (using PKI);
4) the CEM further validates the ESA against ESA information already stored in the ESA Allow list;
5) the ESA passes flexibility offers to the CEM;
6) the CEM informs the DSRSP that the ESA is back online and forwards the ESA flexibility offer.

Figure A.4 – ESA startup (not for first time)



A.2.2 CEM operates in Routine Mode

This use case will be populated following steering group review

A.2.3 CEM responds to a DSRSP flexibility request (single ESA)

A.2.3.1 Aim

The ESA successfully executes a DSRSP energy flexibility request

A.2.3.2 Assumptions

1) The ESA has the capability to report its own power consumption or production, either as periodic instantaneous measurements or as an actual power profile.
2) The ESA has the capability to provide at least three forecast power profiles.
3) The ESA maintains a secure “flexibility actions” log.
4) The CEM maintains a secure “flexibility actions” log.

A.2.3.3 Pre-conditions

1) ESA is installed in premises and subscribed to a DSRSP energy flexibility service.
2) Consumer HAN is operational.
3) DSRSP WAN is operational.

A.2.3.4 Actors and components

1) DSRSP

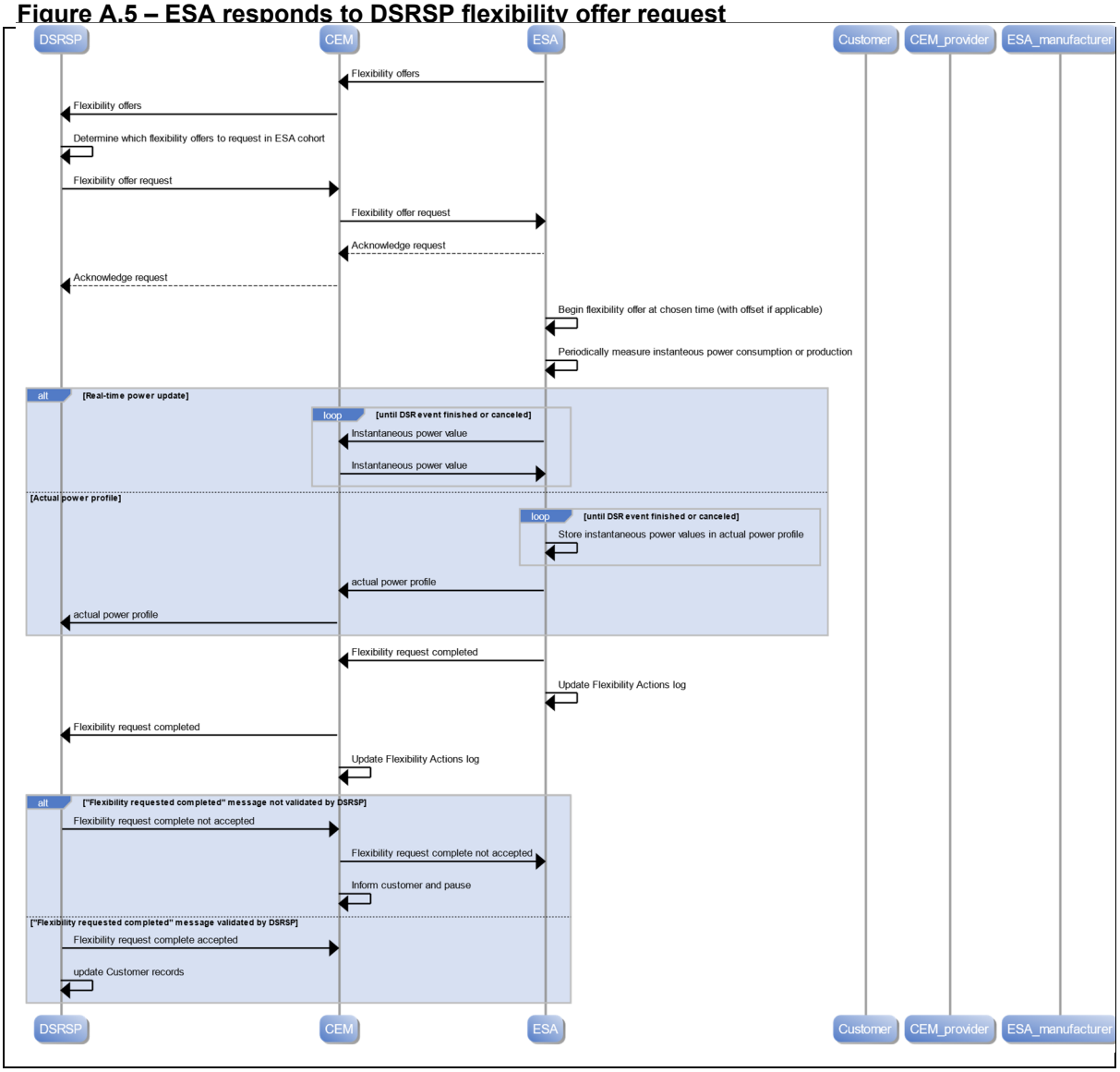
2) Consumer
3) ESA
4) CEM

A.2.3.5 Sequence

An example sequence is listed below and depicted in Figure A.5.

1) The ESA sends its flexibility offers to the DSRSP via the CEM;
2) the CEM receives an “execute flexibility” request from the DSRSP, containing the proposed power profile, a start time and an end time;
3) the CEM acknowledges the “execute flexibility” request with the DSRSP;
4) at the start time the CEM requests the ESA to implement its flexibility offer;
5) the ESA executes the selected flexibility offer;
6) the ESA measures instantaneous power consumption/production values and either sends each value to the DSRSP or logs the values and sends them to the DSRSP in an actual power profile;
7) the ESA sends a “flexibility request completed” message to the CEM, including an identifier for the flexibility request and the start/end energy/power measurement values or “actual used” power profile;
8) the CEM acknowledges the “flexibility request completed” message;
9) the ESA updates its “flexibility actions” log and returns to “Routine” state;
10) the CEM sends a “flexibility request completed” message to the DSRSP, including the identifier for the DSRSP flexibility request and the flexibility provided by the ESA;
    i) the DSRSP validates the “flexibility request completed” message and if acceptable, acknowledges the “flexibility request completed” message;
    ii) otherwise, the DSRSP sends a “flexibility request not acknowledged” message to the CEM;
11) the CEM updates its “flexibility actions” log according to the DSRSP response; and
12) the DSRSP updates the consumer’s flexibility account accordingly; and
13) optionally, the DSRSP sends a message to the consumer, informing them of their recent flexibility contribution (perhaps including consumption or financial information)

Figure A.5 – ESA responds to DSRSP flexibility offer request



A.2.4 CEM responds to a DSRSP flexibility request (via smart meter)

This use case will be populated following steering group review.
It could consider the specific case for an APC in the GB Smart Metering System, or a generic smart metering example.

A.2.5 ESA modifies current ongoing flexibility forecast

A.2.5.1 Aim

The change in ESA power profile is updated within the system.

A.2.5.2 Assumptions

None

A.2.5.3 Pre-conditions

1) The ESA is carrying out a DSR Event in accordance with a flexibility offer chosen by the DSRSP.

2) An ESA's flexibility offers changes during routine or response mode operation(perhaps due to an "active period" in a profile being completed, a consumer intervention, a ToU tariff change or a change in status of another ESA etc.).

A.2.5.4 Actors and components

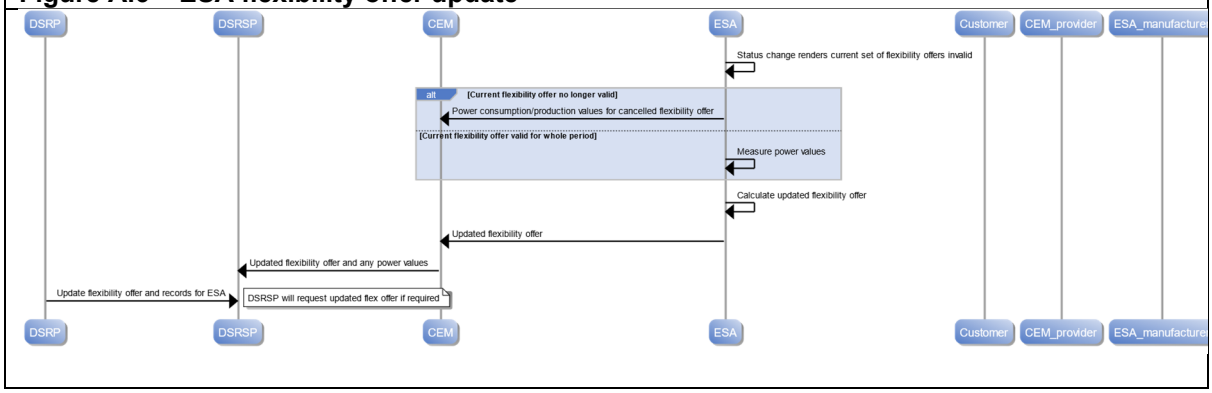
1) DSRSP
2) Consumer
3) ESA
4) CEM
5) ESAG (if present)

A.2.5.5 Sequence

An example sequence is listed below and depicted in Figure A.6.

1) The status of the ESA changes and its current set of flexibility offers is no longer valid;
2) if the currently implemented flexibility offer is no longer valid, then the ESA switches to a new operation immediately (determined by the change in status) and informs the CEM of its power consumption/production accordingly;
3) the ESA calculates a new set of flexibility offers and sends them to the CEM, indicating of the current flexibility offer is still valid or not;
4) the ESA continues to measure its power consumption or production;
5) the CEM passes the new set of flexibility offers to the DSRSP;
6) the DSRSP updates the active flexibility offers for ESA and its records for the ESA; and
7) the DSRSP considers the updated flexibility offers within the context of its ESA cohort and issues a flexibility offer request to the ESA when appropriate.

Figure A.6 – ESA flexibility offer update



A.2.6 CEM operates multiple ESAs

A.2.6.1 Aim

The CEM manages energy flexibility across two or more ESAs.

A.2.6.2 Assumptions

The CEM must be able to consider the flexibility offers of more than one ESA separately may be able to consider an aggregation.

A.2.6.3 Pre-conditions

1) The CEM is connected to more than one ESA.
2) Each ESA has been authenticated with the CEM.
3) the ESAs involved are able to provide flexibility offers.

A.2.6.4 Actors and components

1) DSRSP
2) Consumer
3) ESA#1ESA #2
4) CEM

A.2.6.5 Sequence

Two example options for sequencing with multiple ESAs are depicted in Figure A.7 and Figure A.8.

In the first option, the ESAs are treated entirely separately by the CEM and DSRSP. The flexibility offers from each ESA are treated separately.

In the second option, the flexibility offerings and power values of the ESAs are aggregated by the CEM before being passed on to the DSRSP. The CEM dis-aggregates any flexibility offer request from the DSRSP before passing individual requests to each ESA. This configuration is beyond the scope of this PAS.

Figure A.7 – Multiple ESAs connected to one CEM - non-aggregated

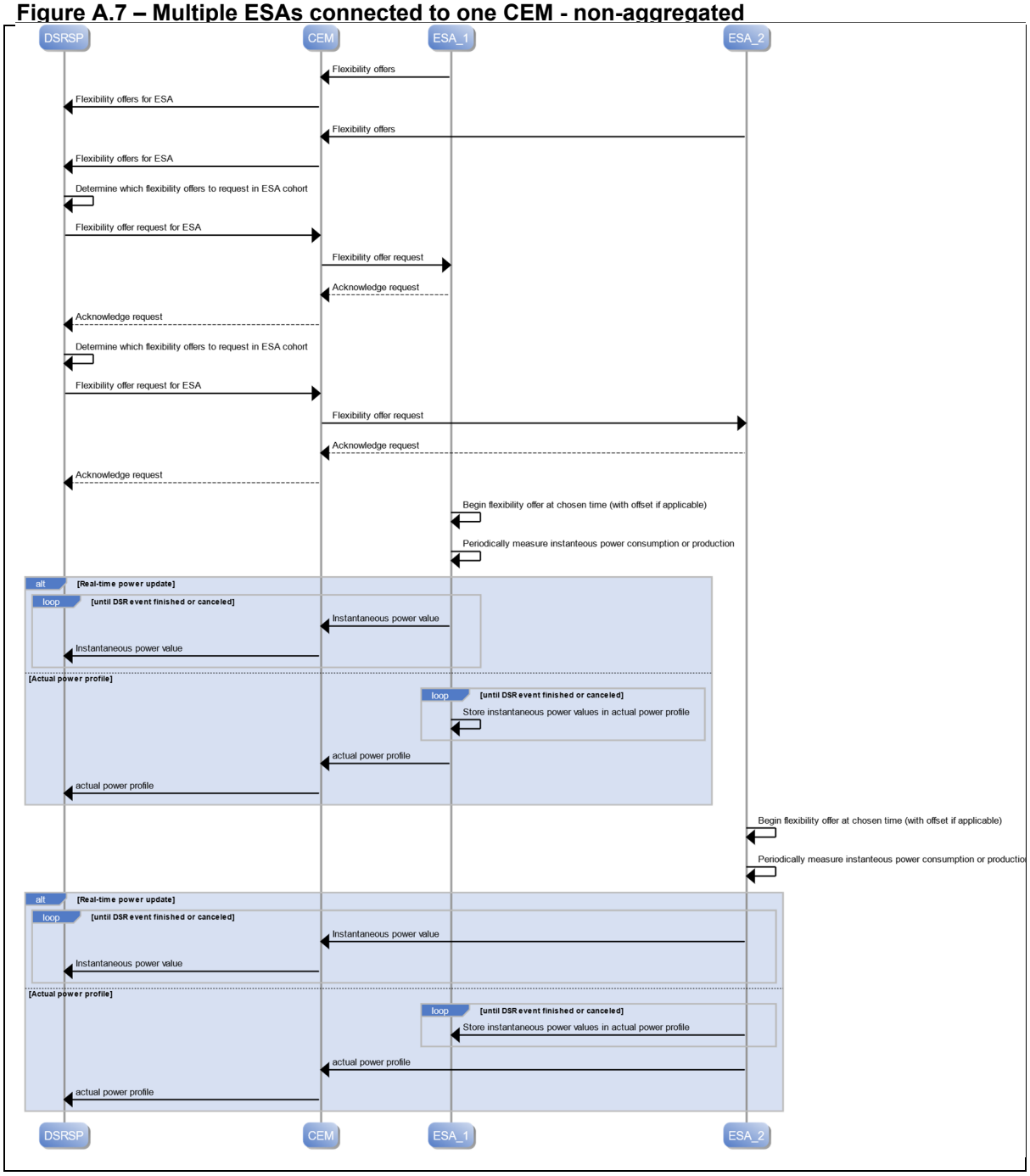
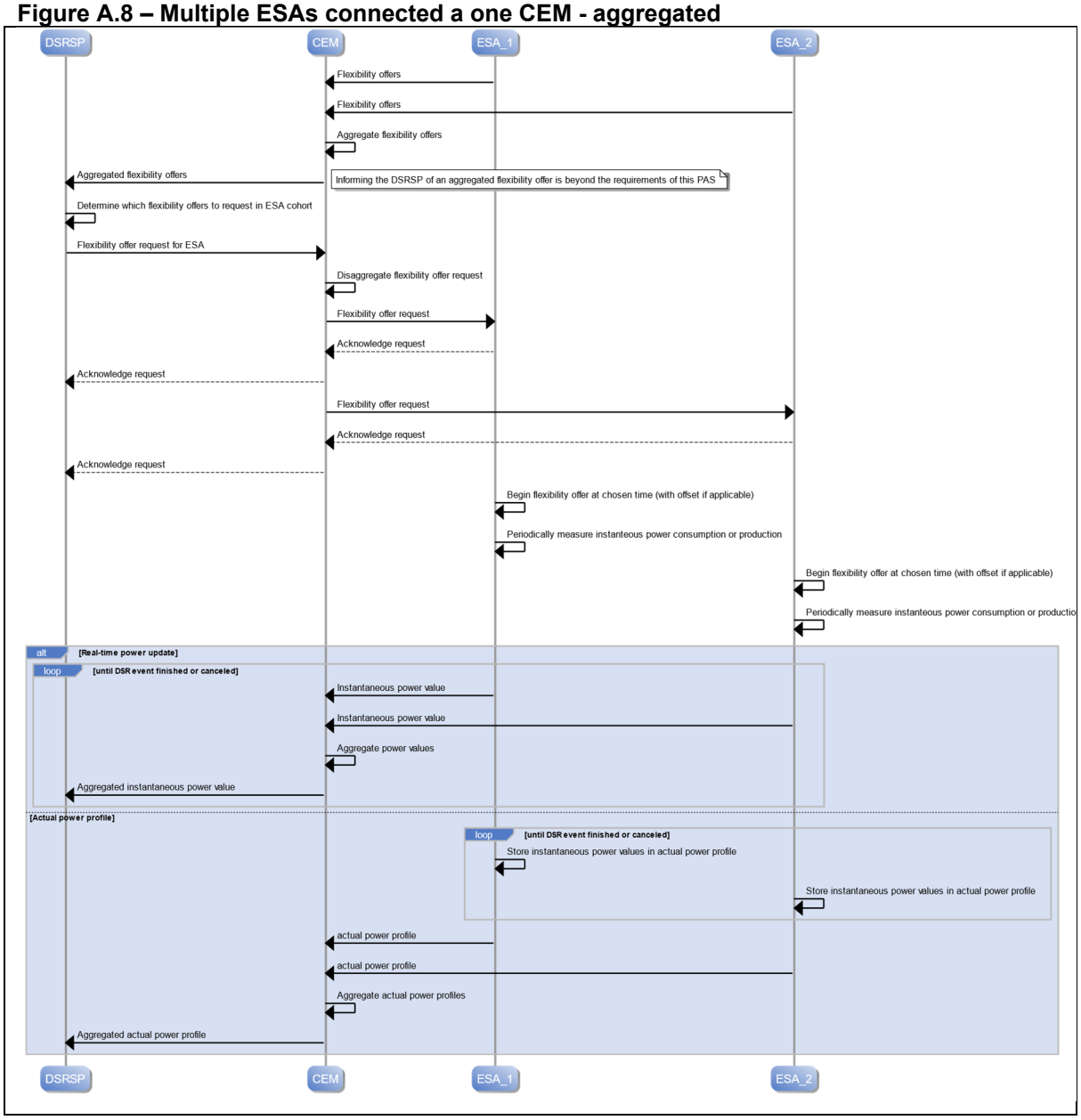


Figure A.8 – Multiple ESAs connected a one CEM - aggregated



A.2.7 Consumer manually over-rides Response or Routine Mode DSR

This use case will be populated following steering group review

A.2.8 Worked example of protocol interoperability

This use case will be populated following steering group review

A.2.9 Worked example of obtaining and using tariff for routine and response mode

This use case will be populated following steering group review.
It could be based on the optional GB Smart Metering use case.
It should be noted that there are many different physical/virtual CEM/ESAG implementations, and how these are implemented will determine how any ESA/external/consumer inputs might be received.

A.3 Specific grid scenario type use cases

A.3.1 Battery storage offers then operates frequency response service in Response Mode for TSO

This use case will be populated following steering group review

A.3.2 Fridge/HVAC operates on IO (based on ToU) in Routine Mode then operates on MD in Response Mode for constraint management for DSO

This use case will be populated following steering group review

A.3.3 EV plugs into chargepoint, calculates profiles and does LD in Response Mode for demand turn up to match high RE on the grid for TSO, then goes into IO operation for Routine Mode after the DSR Event

This use case will be populated following steering group review

A.3.4 ESA and CEM recover from a loss of power to the premises

A.3.4.1 Aim

1) ESA and CEM re-connect to the DSRSP after a power blackout.
2) ESA is once more able to exchange energy flexibility messages with DSRSP and relevant intermediate components.

A.3.4.2 Assumptions

1) All components activate their smart interfaces upon power up.
2) All keys and related authentication and encryption information are securely stored on the component.

A.3.4.3 Pre-conditions

1) ESA and CEM are already authenticated and operating with a DSRSP.

A.3.4.4 Actors and components

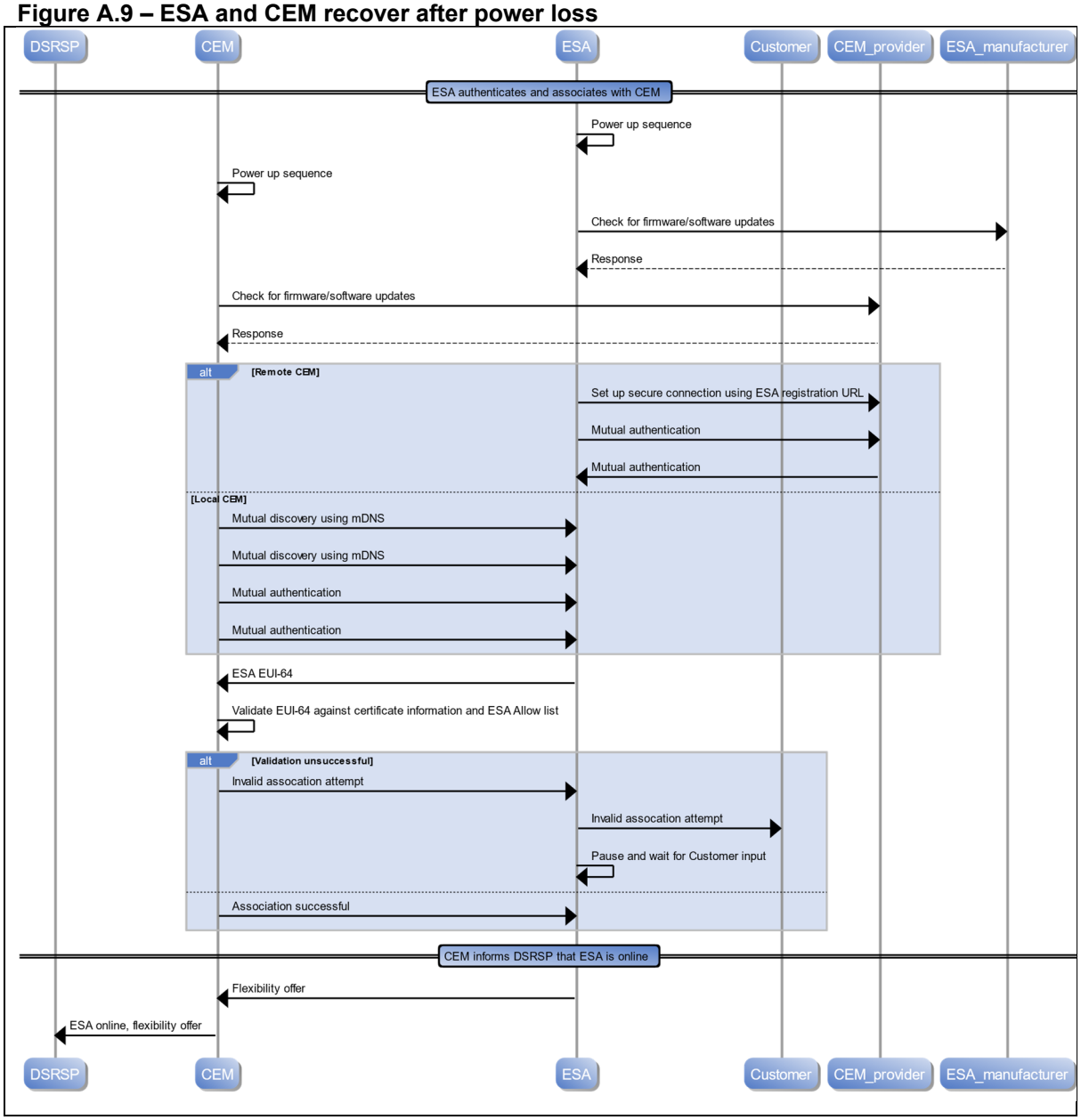
1) DSRSP
2) Consumer
3) ESA
4) CEM

A.3.4.5 Sequence

An example sequence is depicted in Figure A.10. The main steps are:

1) The ESA powers up;
2) the ESA checks for firmware update;
3) The CEM powers up;
4) the CEM checks for firmware update;
5) the ESA and CEM mutually identify and authenticate (using PKI);
6) the CEM further validates the ESA against ESA information already stored in the ESA Allow list;
7) the ESA passes flexibility offers to the CEM;
8) the CEM informs the DSRSP that the ESA is back online and forwards the ESA flexibility offer.

Figure A.9 – ESA and CEM recover after power loss



Annex B (informative)
Implementation examples

*COMMENTARY ON **ANNEX B***

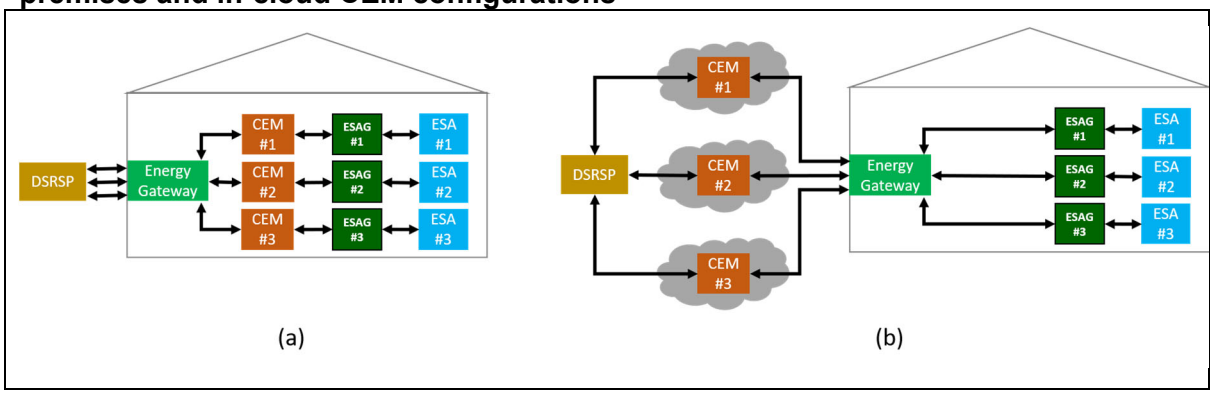
This annex includes examples of how the architecture described in this PAS may be used to achieve various implementation scenarios.

The examples given here provide an initial outline and will be expanded according to input from the SG.

B.1 One DSRSP connects to multiple CEMs, each CEM connected to a single ESA

Figure B.1 shows how a single DSRSP is able to control multiple ESAs in a premises. Example configurations for the CEM placed both in the premises and in the cloud are shown. For the CEM in the cloud case, the ESAG could also be placed in the cloud if required.

Figure B.1 – Single DSRSP controlling multiple ESAs via multiple CEMs for on-premises and in-cloud CEM configurations

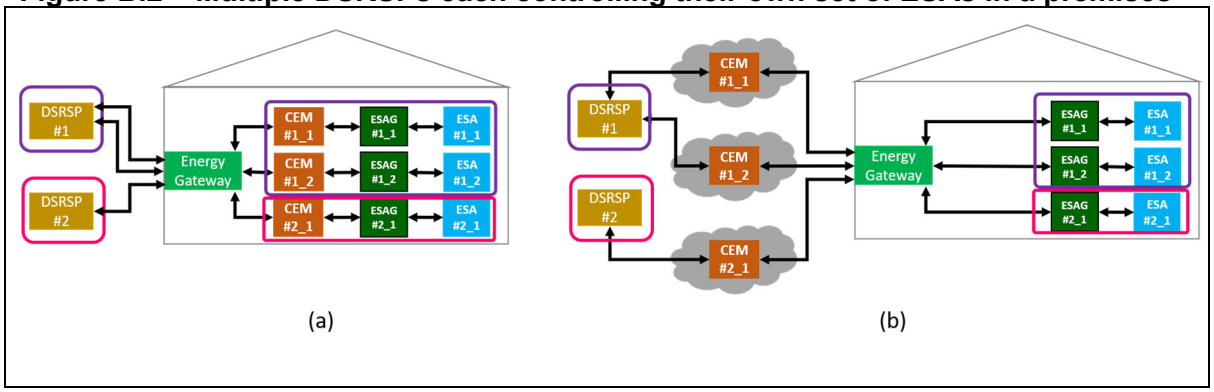


In this example, separate logical communications channels are used for communication between the DSRSP and each of the CEMs. Each channel is subject to its particular authentication and encryption.

B.2 Multiple DSRSPs connect to different CEMs, each CEM connected to a single ESA

Figure B.2 shows example configurations of how multiple DSRSPs are able to control their own particular set of ESAs within the same premises. This is an extension of the case depicted in **B.1** where different DSRSPs make use of different logical channels.

Figure B.2 – Multiple DSRSPs each controlling their own set of ESAs in a premises

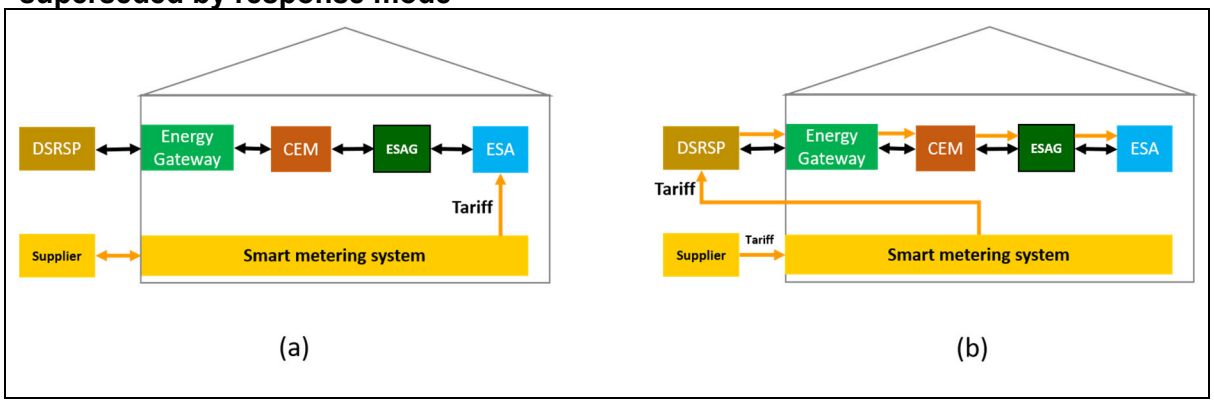


B.3 Routine mode using tariff information is superseded by response mode

Figure B.3 shows two example configurations allowing the ESA or CEM to obtain electricity tariff information and to schedule the operation of the ESA accordingly. In the configuration shown in Figure B.3a), the ESA obtains tariff information directly from the smart metering system in the premises over a HAN connection (other connections are possible). In that

shown in Figure B.3b), the ESA obtains tariff information from the smart metering system, via the DSRSP over a WAN connection. Information on GB smart metering system integration is given in Annex D.

Figure B.3 – ESA operation in routine mode according to electricity tariff is superseded by response mode



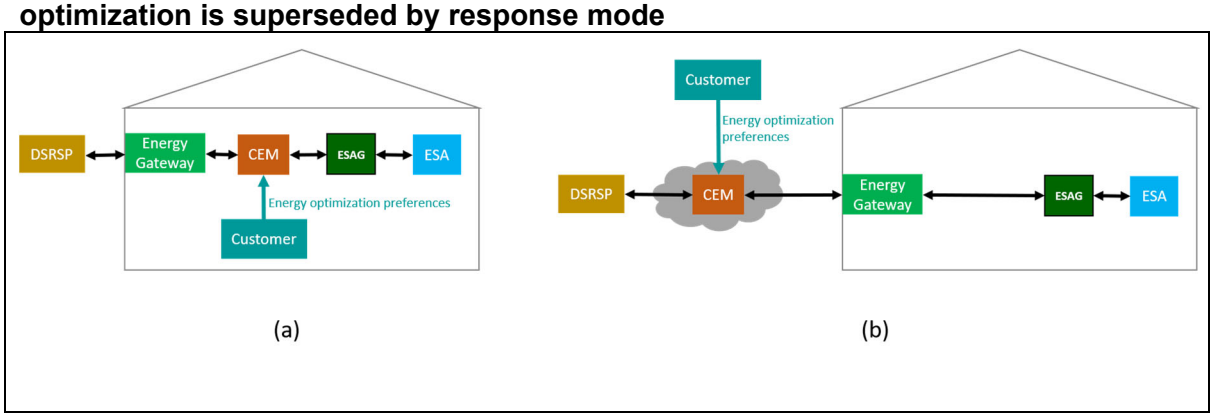
In routine mode, the ESA operates according to user preferences and electricity tariff, e.g. scheduling operations to coincide as far as possible with lower tariffs. During this time, the CEM continues to send ESA forecast power profile updates to the DSRSP.

When the DSRSP sends a flexibility request to the CEM, then the CEM enters response mode and the ESA begins to operate according to the chosen forecast power profile.

B.4 Routine mode using customer preference optimization is superseded by response mode

Figure B.4 shows examples of how the customer is able to provide operating preferences to the CEM, both from a “local” CEM user interface and from a cloud based interface. These preferences are used by the CEM to choose the most appropriate ESA forecast power profiles. During routine mode, the CEM continues to send ESA forecast power profile updates to the DSRSP. When the DSRSP sends a flexibility request to the CEM, the CEM enters response mode and the ESA begins to operate according to the chosen forecast power profile.

Figure B.4 – ESA operation in routine mode according to user preference optimization is superseded by response mode



Annex C (informative)
ESA classification

The information passed across the CEM interfaces does not include any information explicitly stating and classifying the ESA product category, DSR response time or maximum/minimum power limits.

Providing such information to the DSRSP requires additional permissions from the service subscriber, if it is deemed to be personal information.

Nevertheless, DSRSPs might consider such information useful for the delivery of their services.

This annex gives examples of how such additional information could be classified for standardized provision to the DSRSP. The “classifier” values could be sent to the DSRSP during the DSR service registration phase (see Tables C.1, C.2, C.3, C.4).

The need for classification, the categories and association parameters should be agreed by the Steering Group

One possible option for classification of ESAs is basing classification on the product category of the ESA. Table C.1 lists selected examples of ESA product categories as an illustration of the range of products currently suitable for domestic DSR.

Table C.1 – ESA product category classification options

Product category	Product category classifier
Electric HVAC	1
Battery storage	2
Wet appliances	3
Cold appliances	4
Smart EV chargepoint	5

Another, possible option for classification of ESAs is basing classification on the DSR services they can provide. Table C.2 lists selected examples of DSR products as an illustration of the range of products currently common in the UK[1)]. Tables C.3 and C.4 list maximum and minimum power classification options as an illustration of typical ESA power values which could be aggregated to provide DSR services.

[1)] For a list of all NG ESO balancing services, see https://www.nationalgrideso.com/balancing-services/list-all-balancing-services.

Table C.2 – ESA response time classification options

DSR service		Response time	Length of response	Response time classifier
STOR		20 min to 240 min	≥120 min Recovery period <1200 min	A
Non-dynamic (static) FFR	Secondary response	<30 sec	30 min	B
Dynamic FFR	Secondary response	<30 sec	30 min	C
	Primary response	2 sec to 10 sec	20 sec	D
	High response	<10 sec	Indefinitely unless otherwise agreed	E
Non-dynamic (static) EFR	Low Frequency Static	<1 sec	30 min	F
Dynamic EFR	Dynamic Low High (Primary, Secondary and High)	Detection within 500 msec Delivery within 1 sec	Subject to invitation to tender Approximate minimum 15 min Approximate maximum 30min	G
Distribution network constraint management	Generation turn up / Demand turn down	15 min from receipt of dispatch signal	≥60 min	H
Distribution network high voltage substation management	Reduction in imports / Increase in export	30 min from receipt of dispatch signal	≥30 min	I
Distribution network low voltage substation management	Reduction in imports / Increase in export	N/A (scheduled dispatch)	≥30 min	J

Table C.3 – ESA minimum power classification options

Minimum operational power[A)] kW	Minimum power classifier
<(-22)	-5
≤(−22) to (−15)	−4
≤(−15) to (−7)	−3
≤(−7) to (−3)	−2
≤(−3) to 0	−1
0	0
≥0 to 3	1
≥3 to 7	2
≥7 to 15	3
≥15 to 22	4
>22	5

[A)] Negative values are power output; positive values are load.

Table C.4 – ESA maximum power classification options

Maximum operational power[A)] kW	**Maximum power classifier**
≤(−22) to (−15)	−4
≤(−15) to (−7)	−3
≤(−7) to (−3)	−2
≤(−3) to 0	−1
0	0
≥0 to 3	1
≥3 to 7	2
≥7 to 15	3
≥15 to 22	4
>22	5

[A)] Negative values are power output; positive values are load.

Annex D (informative)
Integration with the GB smart metering system

D.1 General

The DSR architecture defined in this PAS functions as a standalone architecture and is also fully technically compatible with the GB smart metering architecture, for provision of DSR services in jurisdictions which have installed smart meters conforming to Smart Metering Equipment Technical Standards (SMETS2). This annex provides information on how this is achieved.

NOTE Further information on technical aspects of GB smart metering can be found in the following references:

- *Latest versions of SMETS (and GBCS) and DCC User Interface Specification [6];*
- *Technical and Business Architecture Documents [7];*
- *DCC User roles [8]; and*
- *Security and privacy obligations overview [9].*

D.2 Architecture overview

D.2.1 Diagram and configurations for DSR modes

D.2.1.1 General

An architectural overview of the DSR system and the relevant components of the GB smart metering system is shown in Figure D.1.

For DSR operations, this architecture can be used in multiple configurations.

For tariff information access the following routes are possible:

- Route 1: tariff over the smart meter HAN, via the ESA;
- Route 2: tariff over the DCC WAN, via the DSRSP.

For load control functionality the following routes are possible:

- Route 3: load control over the SM network, via the APC;
- Route 4: load control over the internet, via the CEM.

NOTE Route 4 does not use the smart metering system but is included for comparison purposes.

These routes are described in the following subclauses.

Routine and response modes of CEM operation can be delivered using any combination of the above routes, i.e. smart metering and non-smart metering routes may be used in conjunction. For example, Route 2 can be used to obtain tariff information over the internet for routine mode alongside using Route 3 to control load over the smart meter HAN (SMHAN) for response mode.

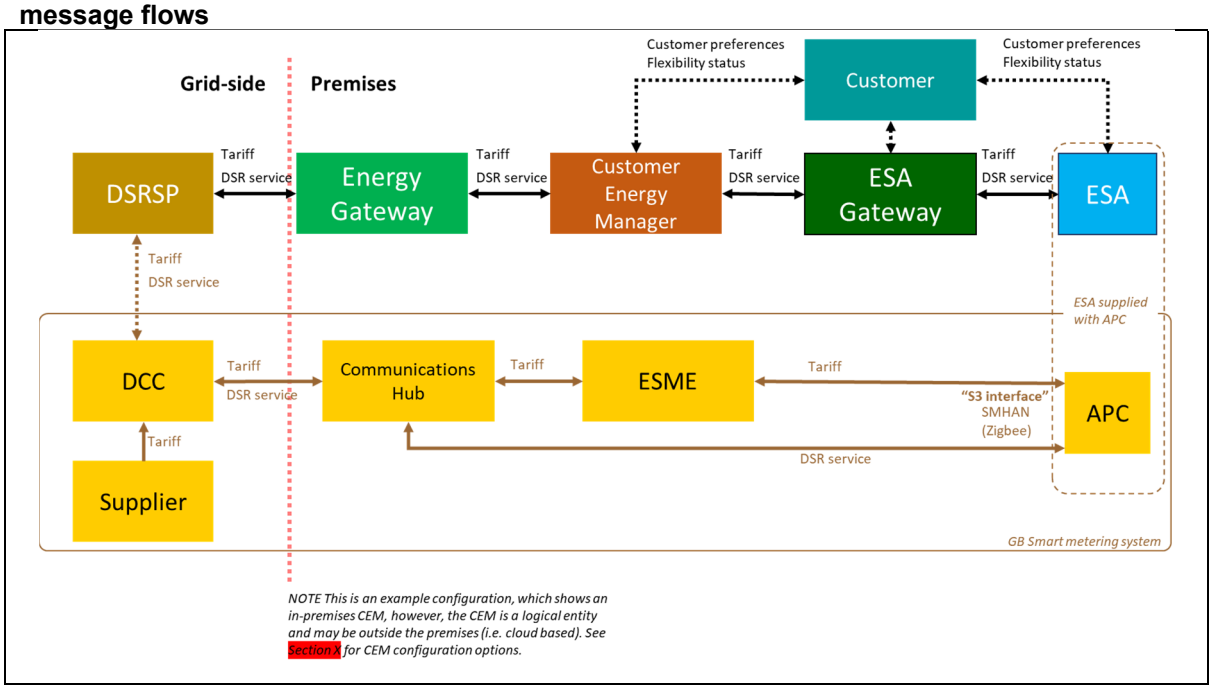
D.2.1.2 Summary of requirements

The components required for each route are summarized as follows:

- Routes 1, 2, 3 and 4 require a CEM/ESAG in order to create power profile options from consumer preferences, external data and appliance information.
- Routes 1 and 2 are the only routes which require an ESME.
- Routes 1, 2 and 3 require a communications hub.
- Route 3 is the only route which requires an APC.
- Routes 1 and 3 require the ESA to be paired to the SMHAN and joined to the ESME by a DCC user.

- Routes 2 and 3 require the DSRSP to be a DCC User in the user role of “Import Supplier”.

Figure D.1 – Overview of DSR and GB smart metering architectures, showing high level message flows



D.2.2 Components description

NOTE The following components are part of the GB Smart Metering System architecture.

D.2.2.1 DSRSP

As defined in **3.1.12** and **3.1.13**, a DSRSP operates ESAs, in line with consumer wishes, to provide DSR services to grid-side actors. Specific DSRSP requirements, such as the DCC user role required for operation, are described under individual routes in **D.3.2**, **D.3.3**, **D.4.2** and **D.4.3**.

D.2.2.2 Import supplier

Import supplier is a DCC user role. It is the only DCC user role that can undertake activities such as setting the tariff on the ESME and sending/receiving messages to/from the load control functionality of the smart metering system. “Import Supplier” and ”supplier” can be taken to have the same meaning.

D.2.2.3 DCC

DCC (Smart DCC) has built and maintains the secure national infrastructure that underpins the roll-out of smart meters across Great Britain. This wireless network connects smart meters to energy suppliers, network operators and other authorized service users. It is maintained to very high security standards, as endorsed by the National Cyber Security Centre.

D.2.2.4 Communications hub

The communications hub is a device described by the Communications Hubs Technical Specifications [12]. Its principal functions are:

- acting as an interface between DCC WAN and SMHAN;
- acting as SMHAN coordinator; and

- providing a backup for gas data.

D.2.2.5 ESME

The ESME is a device described by the Smart Metering Equipment Technical Specifications [11]. Its principal functional areas are:

- metering;
- credit and prepayment payment modes;
- ToU and block tariffs;
- network monitoring; and
- storage of consumption data.

D.2.2.6 Auxiliary proportional controller (APC)

The auxiliary proportional controller (APC) is an optional functionality that can be used as part of an ESME or as part of a standalone auxiliary proportional controller (SAPC). The principal functional areas are:

- the Import Supplier can set an output level of 0 to 100 in 0.1 increments;
- the APC can provide event driven information (“alerts”) to the Import Supplier about a load to which it is connected;
- the Import Supplier can set information on the APC about the load to which the APC is connected; and
- the Import Supplier can retrieve information logged by the APC about the load to which the APC is connected.

An SAPC can contain a maximum of five APCs. An ESME can contain a maximum of five APCs. A communications hub can support a maximum of any combination of up to four SAPCs or ESMEs, e.g. one communications hub can support one ESME and three SAPCs.

The full technical specification of APC-related functionality is described in SMETS2 version 5 [12] and later.

The other components are part of the DSR architecture, as described in Clause **4**.

D.3 Tariff information via GB smart metering system

D.3.1 Tariff information access

The tariff information available from the smart metering system comprises prices and times and dates/consumption (“block”) thresholds for which the prices are active. This tariff information can be used to construct power profiles for DSR operation.

The smart metering system is used to deliver tariff information to the CEM/ESAG. The smart metering system can be used to deliver this information in two configurations:

- Route 1: tariff over the SMHAN, via the ESA; or
- Route 2: tariff over the DCC WAN, via the DSRSP.

These routes are described in D.3.2 and D.3.3.

NOTE For this interoperable DSR architecture, the tariff information cannot be obtained via an internet/SMHAN bridge device (i.e. CAD), because there is no standardized protocol or data model for the internet side of the bridge.

D.3.2 Route 1: Tariff information via SMHAN

D.3.2.1 Process flow

The process flow is as follows.

- The tariff information is set on the ESME by the supplier.
- The supplier passes tariff information for a customer to the DCC.
- The DCC routes the tariff information to the ESME, via the communications hub and SMHAN, in the customer's premises.
- The tariff information is made available over the SMHAN and the ESA supports a Zigbee SE interface to read this information.
- The ESA passes the tariff information to the CEM/ESAG, via the S2 interface.
- The CEM/ESAG uses the tariff information to create power profiles for routine and response mode operation, which are then passed to the DSRSP.

The requirements for power profiles and updates are set out in **5.4**.

D.3.2.2 Summary of requirements

The main requirements for Route 1 are summarized below:

- In order to support this configuration, the ESA incorporates a Zigbee SE interface – the so-called "S3" interface. Additionally, the ESA is paired to the SMHAN and joined to the ESME by a DCC user (e.g. DCC user roles Import Supplier, "other user", etc.)
- A CEM/ESAG is used to create power profile options from consumer preferences, external data and appliance information.

NOTE The system architecture and message flow for this configuration is shown in Figure D.2 and Figure D.3 respectively.

Figure D.2 – Functional architecture for routine mode using Route 1: Tariff information via SMHAN (e.g. ESA is ZigBee SE enabled)

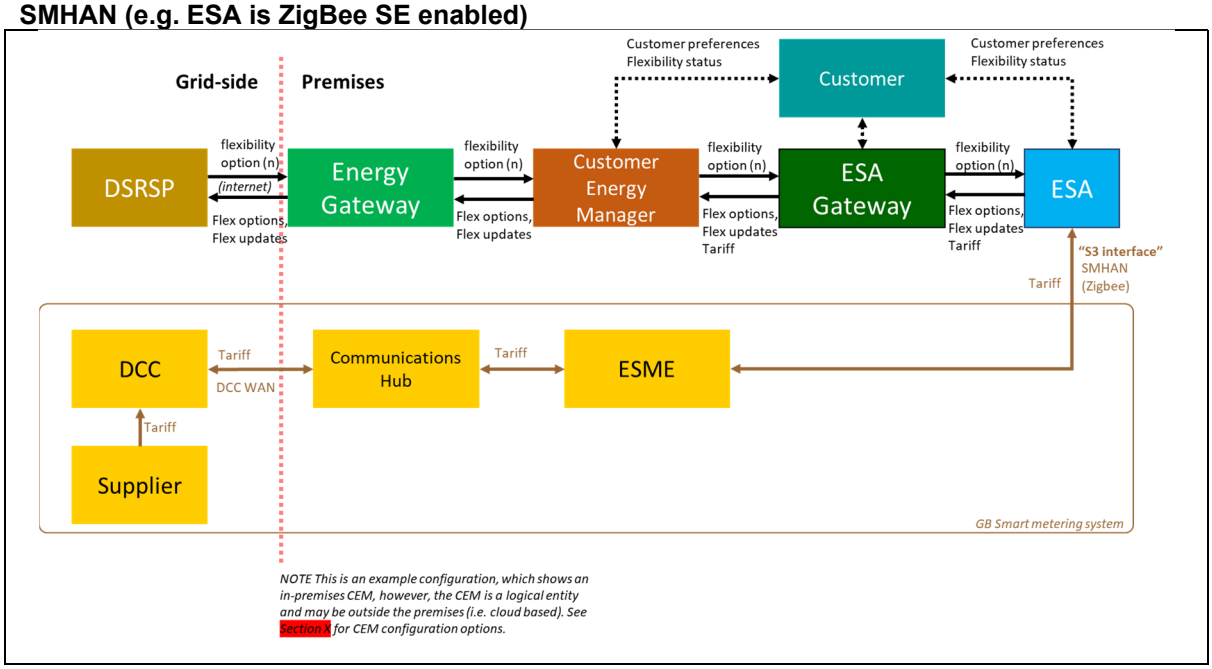


Figure D.3 – Message flow for routine mode using Route 1: Tariff information via SMHAN (e.g. ESA is ZigBee SE enabled)

To be added following public consultation.

D.3.3 Route 2: Tariff information via DCC WAN

D.3.3.1 Process flow

The process flow is as follows.

- The tariff information is set on the ESME by the supplier.
- The Supplier passes tariff information for a customer to the DCC.
- The DCC routes the tariff information to the ESME, via the communications hub and SMHAN, in the customer's premises.
- The tariff information is read from the ESME by the DSRSP, via the communications hub and the DCC.
- The DSRSP passes the tariff information to the CEM/ESAG, via the S1 interface, and the ESA is internet enabled to read this information.
- The CEM/ESAG use the tariff information to create power profiles for routine and response mode operation, which are then passed to the DSRSP.

The requirements for power profiles and updates are set out in **5.4**.

D.3.3.2 Summary of requirements

The main requirements for Route 2 are summarized below:

- In order to support this configuration, the DSRSP is a DCC user in the user role of "Import Supplier".
- The ESA is not required to have an S3 interface.
- A CEM/ESAG is required to create power profile options from consumer preferences, external data and appliance information.

NOTE The system architecture and message flow for this configuration is shown in Figure D.4 and Figure D.5 respectively.

Figure D.4 – Functional architecture for routine mode using Route 2: Tariff information via DCC WAN (e.g. ESA is internet enabled)

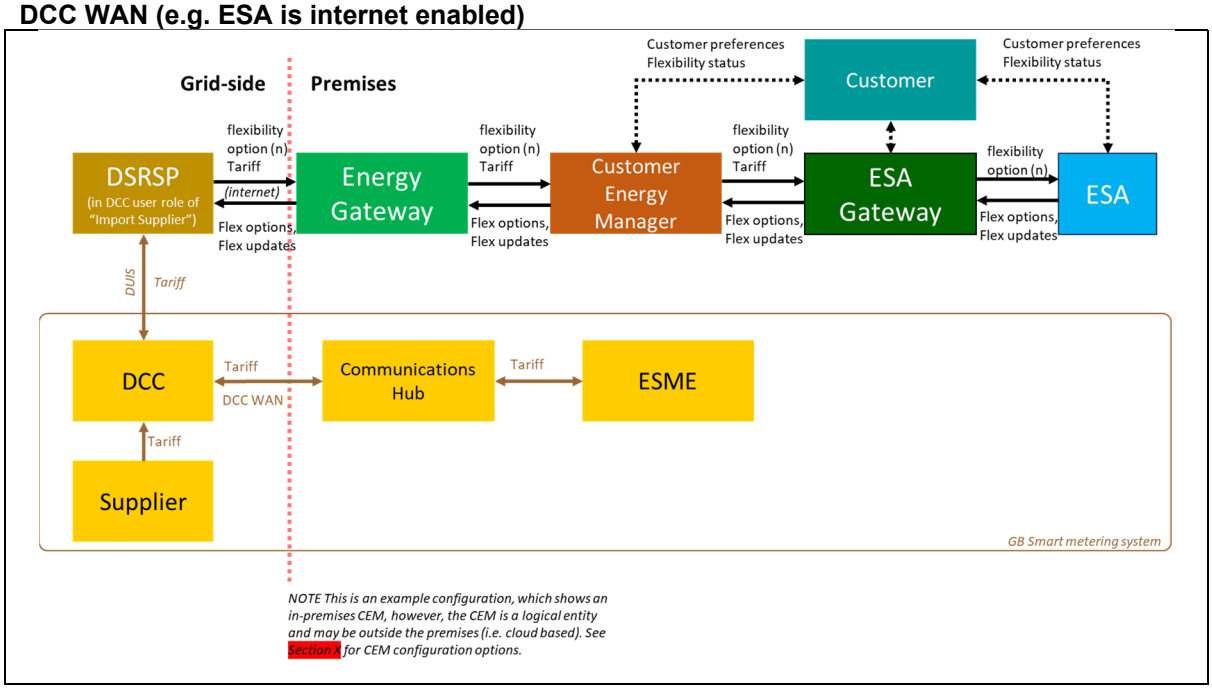


Figure D.5 – Message flow for routine mode using Route 2: Tariff information via DCC WAN (e.g. ESA is internet enabled)

To be added following public consultation.

D.4 Load control via GB smart metering system

D.4.1 Load control functionality

The load control functionality available from the smart metering system is provided by the APC device. In order to deliver this functionality, the ESA is supplied with an APC interface (the interface between the ESA and APC is not specified); this combination is now referred to as “ESA/APC”. The ESA/APC is paired to the SMHAN and the ESA/APC can then be operated by a DSRSP in the DCC user role of Import Supplier.

The ESA/APC facilitates the reporting of available power profiles and the selection of a specific power profile by the DSRSP for response mode operation, via the communications hub and the DCC.

In this configuration, each power profile is uniquely numbered, and the power profile and corresponding number can be supplied to the DSRSP via the smart metering system (Route 3) or via the DSR architecture (Route 4). An APC can receive a number between 0 and 100 (in 0.1 increments), which can correspond to a unique power profile number sent to/from the ESA/APC.

The smart metering system can optionally be used for ESA load control. Using the smart metering system only, this can be achieved in one configuration: Route 3: load control via APC.

NOTE 1 For completeness, ESA load control can also be achieved without using the smart metering system in one configuration: Route 4: load control via CEM.

NOTE 2 Route 4: load control via CEM can be used in conjunction with Route 3, e.g. Route 4 to send power profile options and Route 3 to select a specific power profile, or it can be used as an alternative to Route 3. These routes are described in D.4.2 and D.4.3.

*NOTE 3 For this DSR architecture, load control cannot be achieved using ALCS and HCALCS devices, as they do not have the functionality to support the operation of power profiles specified in **5.4.4.1**.*

D.4.2 Route 3: Load control via APC

D.4.2.1 Process flow

The process flow is as follows.

- The ESA is supplied with an APC.
- The CEM/ESAG creates power profiles, each with unique numbers, for routine and response mode operation, and sends them to the ESA/APC, via the S2 interface.
- The ESA/APC sends the information to the DSRSP as an event-based alert, via the S3 interface.
- The information is passed over the SMHAN to the communications hub, which passes the information over the WAN to the DCC and onto the DSRSP.
- During response mode, the DSRSP selects a power profile and sends the corresponding unique number to the ESA/APC.
- The DSRSP passes the number to the DCC, which routes the number to the ESA/APC, via the S3 interface, using the communications hub and SMHAN.
- The ESA/APC implements operation of the corresponding power profile.
- The ESA/APC sends the number to the CEM/ESAG, which updates the power profiles accordingly and sends the updated profiles to the DSRSP via the same route above (see also caveat in the following bullet point).
- The sending of the specific power profile number to the ESA/APC only occurs via Route 3 in this configuration. However, both the initial provision of power profiles and numbers to the DSRSP, and the subsequent updating of power profiles and numbers from the ESA/APC to the DSRSP, can occur either via Route 3 or Route 4.

D.4.2.2 Summary of requirements

The main requirements for Route 3 are summarized below:

- In order to support this configuration, the ESA is supplied with an APC interface. The provision of an APC interface means the ESA/APC has a Zigbee SE interface – the so-called “S3” interface. Additionally, the ESA/APC is paired to the SMHAN and joined to the ESME by a DCC user (e.g. DCC user roles: Import Supplier, “other user”, etc.).
- In order to support this configuration, the DSRSP is a DCC user in the user role of Import Supplier.
- A CEM/ESAG is required in order to create power profile options from consumer preferences, external data and appliance information.

NOTE 1 There is no mandatory connection between the CEM/ESAG and DSRSP. This is because DSR messages could pass between the DSRSP and CEM via the components of the smart metering architecture, the ESA and ESAG.

NOTE 2 The system architecture and message flow for this configuration is shown in Figure D.6 and Figure D.7 respectively.

Figure D.6 – Functional architecture for response mode using Route 3: Load control via APC (e.g. ESA supplied with APC)

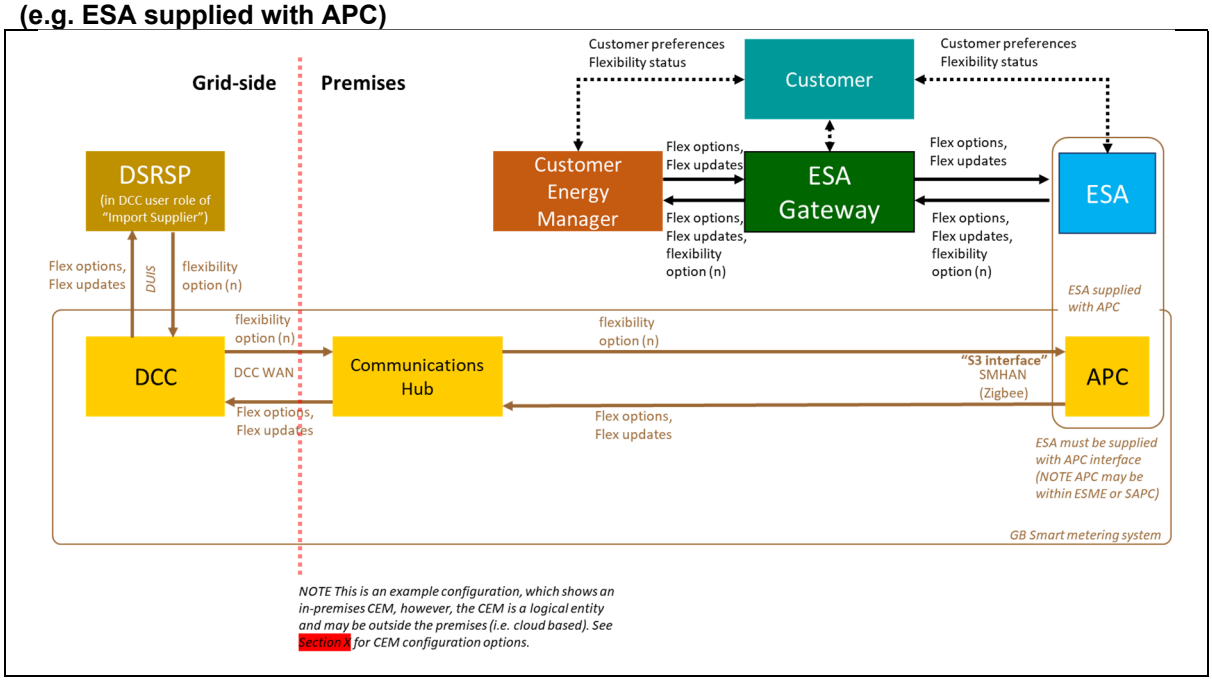


Figure D.7 – Message flow for response mode using Route 3: Load control via APC (e.g. ESA supplied with APC)

To be added following public consultation.

D.4.3 Route 4: Load control via CEM (for completeness)

*COMMENTARY ON **D.4.3***

This route does not utilize the GB smart metering system but is included for completeness as it can be used in conjunction with Routes 1, 2 and 3.

In this configuration, DSR messages are passed between the DSR architecture components as described in Clause **6** and **D.1**.

Annex E (informative)
ESA specification summary

This section will be used to summarise the minimum functional requirements of an ESA.

SG comments on the usefulness of this section are welcomed, this section can be removed if deemed unnecessary.

Summary of ESA requirements:

- minimum attribute 1
- minimum attribute 2

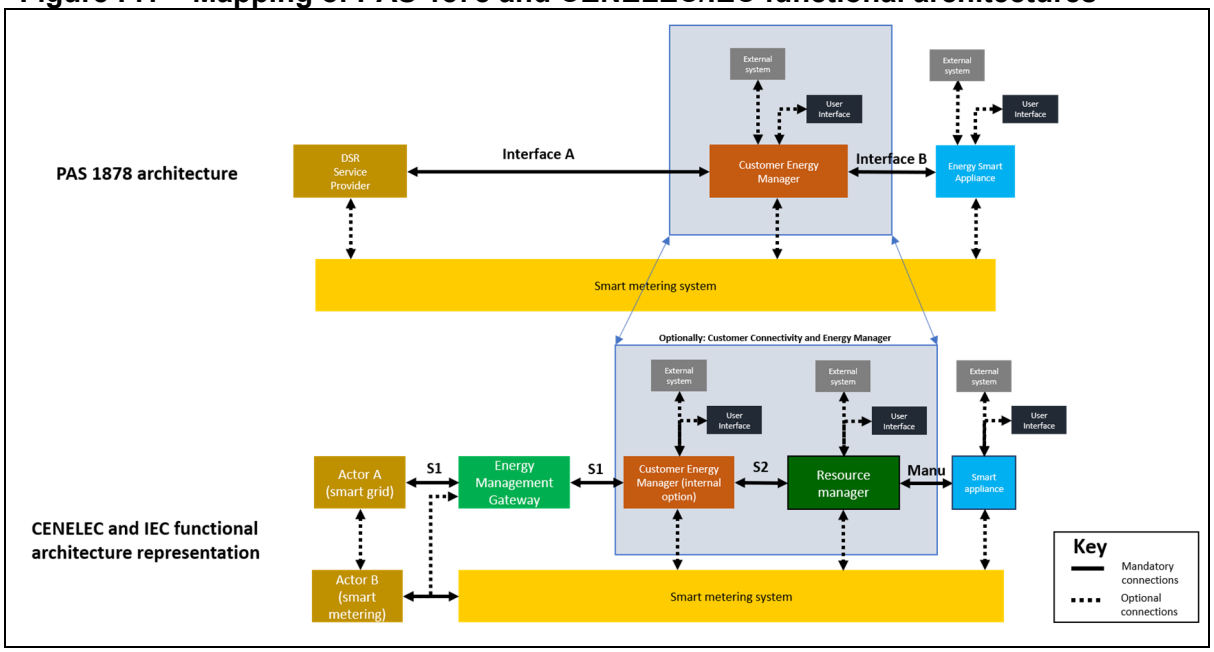
Annex F (informative)
Relationship between the PAS functional architecture and representative CENELEC/IEC functional architecture

*COMMENTARY ON ANNEX **F***

This annex provides information on the relationship between the functional architecture described in this PAS and an amalgamation of the "smart grid" functional architecture included in several CENELEC and IEC standards. The representations in the CENELEC and IEC documents, whilst broadly similar, do differ slightly, hence the need for an amalgamated representation.

The two architectures and how they are mapped are shown in Figure F.1. The CENELEC/IEC architecture is configured assuming that the CEM is internal to the customer premises. As this is a functional architecture, a configuration with the CEM external to the customer premises (e.g. in the cloud) is also permissible.

Figure F.1 – Mapping of PAS 1878 and CENELEC/IEC functional architectures



F.1 Description of CENELEC/IEC components and interfaces

NOTE Figure F.1 shows the relationship between the PAS 1878 functional architecture and an amalgamated representation of the smart grid flexibility functional architecture depicted in several CENELEC and IEC standards, including EN 50491-12-1, EN 50631-1, [1], IEC TR 62746-2, and prEN50491-12-2.

F.1.1 Smart appliance

The Smart appliance is device that is able to consume, produce or store energy and that is connected to an external energy-related management entity. EN 50631-1 states that this connectivity occurs using a "Device Connection Manager", a necessary requirement for the appliance becoming "smart".

F.1.2 Resource Manager

This occurs in BS EN 50491-12-1, prEN50491-12-2 and is implicitly included in the Customer Connectivity and Energy Manager (CCM) of BS EN 50631-1. From BS EN 50491-12-1, *"software component that exclusively represents a logical group of devices or a single smart device, and is responsible for sending unambiguous instructions to the logical group of devices or to a single device, typically using a device-specific protocol".* Its main task is to convert between the manufacturer specific protocols used by the Smart appliance and the (to be) standardized protocol with the CEM (data model defined in prEN50491-12-2). The remaining functionality of the Resource Manager is yet to be fully defined and agreed.

F.1.3 Customer Energy Manager

From BS EN 50491-12-1. “internal automation function for optimizing the energy consumption, production and storage within the premises according to the preferences of the customer using internal flexibilities and typically based on external information received through the Smart Grid Connection Point and possibly other data sources”.

The main task of the CEM is to relay messages between the grid-side Actors A and B and the Resource Manager. It might aggregate flexibility capabilities of different smart appliances or different Resource Managers, generate smart appliance operation schedules based on customer preferences, tariffs, DSR requests etc. The remaining functionality of the CEM is yet to be fully defined and agreed.

F.1.4 Energy Management Gateway

This component acts as a communications access point, allowing information to be exchanged between the Customer Energy Manager and the two grid-side actors A and B. In some architectures, it also acts as a gateway to the smart metering system.

F.1.5 Actor A

Actor A is a blanket term for any entity, or combined entities, on the grid-side (for example an aggregator, DSO, DNO or TSO) responsible for operating grid services interacting with the customer premises (for example to deliver DSR).

F.1.6 Actor B

Actor B is a blanket term for any entity, or combined entities, responsible for the delivery of smart metering services to the customer premises.

F.1.7 Interface “Manufacturer”

This interface connects the smart appliance to the Resource Manager (or the Customer Connectivity and Energy Manager, in accordance with BS EN 50631-1). The specification of this interface is determined by the appliance manufacturer. Candidates for this interface include that defined in EN 50631-1, Zigbee, Echonet, proprietary implementations, etc.

F.1.8 Interface “S2”

S2 connects the Resource Manager with the Customer Energy Manager. This interface is described in EN 50491-12-1. For the case when this interface connects two separate devices, interoperability between difference devices is seen as key, in order to allow Resource Managers and CEMs from different manufacturers to work with each other. The data model for this interface is being standardized in EN 50491-12-1. In EN 50631-1, this is a software interface internal to the Customer Connectivity and Energy Manager and so is not required to be standardized.

F.1.9 Interface “S1”

S1 connects the CEM, via the Energy Management Gateway, to Actor A and optionally Actor B. Interoperability is a key aspect of this interface, to allow any Actor A to communicate with any CEM. Possible candidates include the IEC 61850 series, IEC 62746-10-1: 2018, EEBus or the development of a new standard. There is currently no agreement on the specification of S1.

F.2 Mapping of components and interfaces

NOTE From the descriptions in F.1, the equivalent relationships depicted in Table F.1 may be derived. The mapping between the PAS 1878 and CENELEC/IEC components and interfaces are described in the following sections.

Table F.1 – Equivalence between PAS 1878 and CENELECL/IEC functional architectures

PAS 1878	CENELEC/IEC
Energy Smart Appliance	Smart Appliance
Customer Energy Manager	Customer Energy Manager Resource Manager Or Customer Connectivity and Energy Manager
On-premises router/gateway, mobile data modem on ESA or CEM etc.	Energy Management Gateway
DSR Service Provider	Actor A (smart grid)
Smart metering system	Smart metering system Actor B (smart metering)
Interface B	Manufacturer interface
Internal CEM interface (optional)	Interface S2
Interface A	Interface S1

F.2.1 Smart Appliance

The PAS 1878 ESA is very similar to the smart appliance. interface B represents a sub-set of the Device Connection Manager of EN 50631-1. The main difference is that the ESA is currently applied to a defined set of appliance types in this PAS, whereas the smart appliance is not.

F.2.2 Resource Manager

A separate Resource Manager is not a fundamental requirement within PAS 1878 and the CEM is optionally able to take on this role.

This PAS does not restrict the use of a separate Resource Manager

F.2.3 Customer Energy Manager

The CEM in PAS 1878 is equivalent to the “energy manager” functionality of the “Customer Connectivity and Energy Manager” of EN 50631-1, in that it does not deal with non-energy (non-DSR) related communication. This is equivalent to the CEM of EN 50491-12-1.

F.2.4 Energy Management Gateway

The Energy Management Gateway is not explicitly described in PAS 1878. Rather the communication flows between Actors A and B and the premises are treated separately, through Routine Mode and Response Mode operation. Also, requirements are placed upon the external interface in PAS 1878. In the amalgamated architecture, no additional requirements are placed upon the means of communication between Actors A and B and the CEM, allowing any suitable physical layer approach to be taken.

F.2.5 Actor A

Actor A is equivalent to the DSRSP.

F.2.6 Actor B

Actor B is equivalent to the smart metering operator. In the GB specific case, this is equivalent to the DCC and Supplier.

F.2.7 Interface “manufacturer”

This is equivalent to Interface B. Certain information model, messaging and cyber-security requirements are specified in PAS 1878, in order to support DSR operations. However, the details of the data model and underlying protocols are left to the manufacturer.

F.2.8 Interface S2

There is no requirement for an interoperable S2 interface described in PAS 1878. Although this is seen as further work, there is no restriction on the possible optional implementation of S2.

F.2.9 Interface S1

This is equivalent to Interface A. As Interface A is specified in PAS 1878, it is hoped that the definition will contribute to the international standardization of S1.

Annex G (informative)
OpenADR

COMMENTARY ON ANNEX G

This Annex provides an overview of the OpenADR ecosystem and technical specifications. It is entirely informative and attempts to provide information on a best effort basis. Examples are provided for illustrative purposes only. The reader should return to the references for any definitive information.

G.1 Specifications and standardization

OpenADR specifications[1)] are currently at version 2.0 and are formed of two profiles. Profile A (OpenADR2.0a) is designed for resource-constrained, low-end embedded devices that can support basic DR services and markets. Profile B (OpenADR2.0b) is more feature rich and is designed for high-end embedded devices that can support most DR services and markets. Profile B includes a flexible reporting (feedback) mechanism for past, current and future data reports.

OpenADR was active in the Energy Interoperation Technical Committee of OASIS (Organization for the Advancement of Structured Information Standards). OpenADR 2.0 is a profile of OASIS Energy Interoperation 1.0 published in 2014 [16] which is available free of charge from the OASIS website at http://docs.oasis-open.org/energyinterop/ei/v1.0/energyinterop-v1.0.html.

OpenADR 2.0b was published as an IEC International Standard, IEC 62746-10-1:2018 *Systems interface between customer energy management system and the power management system - Part 10-1: Open automated demand response,* in 2018 by IEC TC57 "Power systems management and associated information exchange". The content of this standard is the same as the OpenADR 2.0b specification published on the OpenADR website.

A related standard covering the compatibility of OpenADR with the Common Information Model (CIM) [2], IEC 62746-10-3:2018 *Systems interface between customer energy management system and the power management system – Part 10-3: Open automated demand response - Adapting smart grid user interfaces to the IEC common information model*, also published by IEC TC57.[2)]

To date, no mapping of OpenADR 2.0 onto SAREF (Smart Appliances Reference Ontology) or SAREF4ENER ETSI TS 103-410-1 v1.1.1: 2017 *SmartM2M; Smart Appliances Extension to SAREF; Part 1: Energy Domain* [12] has been performed. SAREF (and its extensions) is a tool that allows the mapping between different data models to be performed at design time.

G.2 Take-up and ecosystem

Management and certification of OpenADR is performed by the OpenADR Alliance [4], at https://www.openadr.org/. The website states that there are currently more than 150 members, with a recent increase in EV charging related companies.

The website lists over 200 OpenADR certified products across the OpenADR system, from cloud based products such as Aggregator packages to end points including several energy management and gateway devices.

The traditional OpenADR installation base has been in North America and the Far East (primarily Japan) although the website does state that there is now activity in Europe. According to the FAQ at [4], "*Over 60 utilities and controls vendors have already announced or deployed OpenADR-based systems across the U.S. and internationally*". It seems that take up in UK and Europe is currently quite low although "interest/in development" level

---

1) The specifications and supporting material are freely available from the OpenADR Alliance website at https://www.openadr.org/specification.

2) IEC TC57 Dashboard

activity is listed in Ireland, Spain and France in addition to mentioning that in the UK the ENA mentioned OpenADR in their DSO Roadmap.

OpenADR systems can be connected to other protocols through gateways. OpenADR has been shown to work with the Open Charge Point Protocol (OCPP) and the Energy Flexibility Interface (EFI) (specified by the FlexiblePower Alliance Network (FAN) and used as one of the foundations of the EN50491-12-x standards from CENELEC).

G.3 System overview

OpenADR forms a platform to pass messages between two primary actors or entities – "Virtual Top Nodes" (VTN) and "Virtual End Nodes" (VEN).
A VTN is responsible for:

- Managing Resources
- Creating/Transmitting "Events"
- Requesting and receiving "Reports"

A VEN is responsible for:

- Receiving "Events" and responding to them
- Generating "Reports"
- Control demand side resources

The architecture is hierarchical in that an intermediate entity may be both a VEN and a VTN. Figure G.1 shows the message passing concept, the hierarchical nature of the OpenADR architecture. Figure G.2 shows a possible mapping between an OpenADR architecture and an example ESA system architecture.

Figure G.1 – OpenADR message and architecture topology concepts

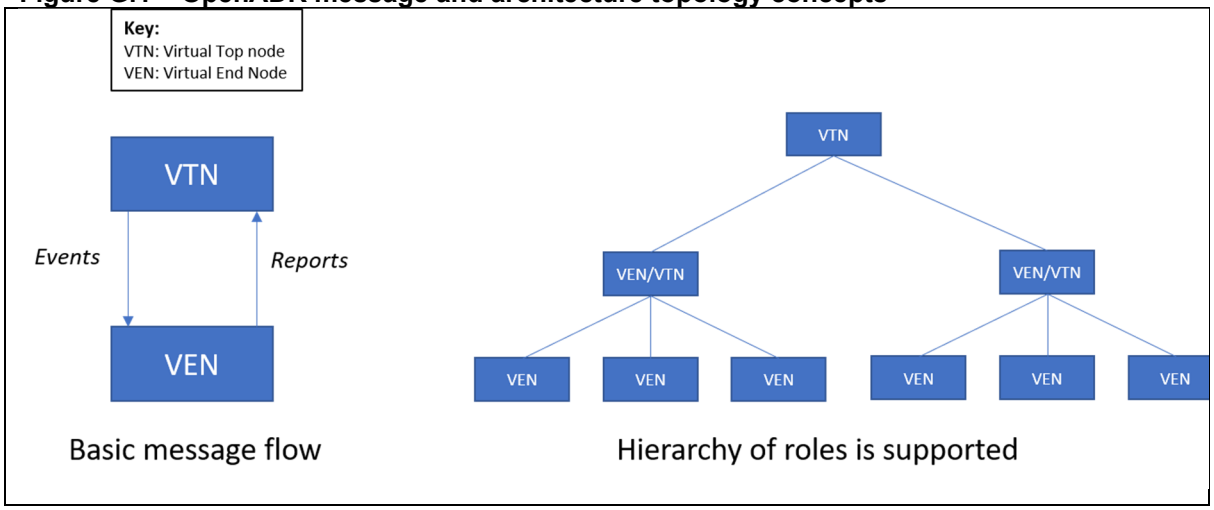
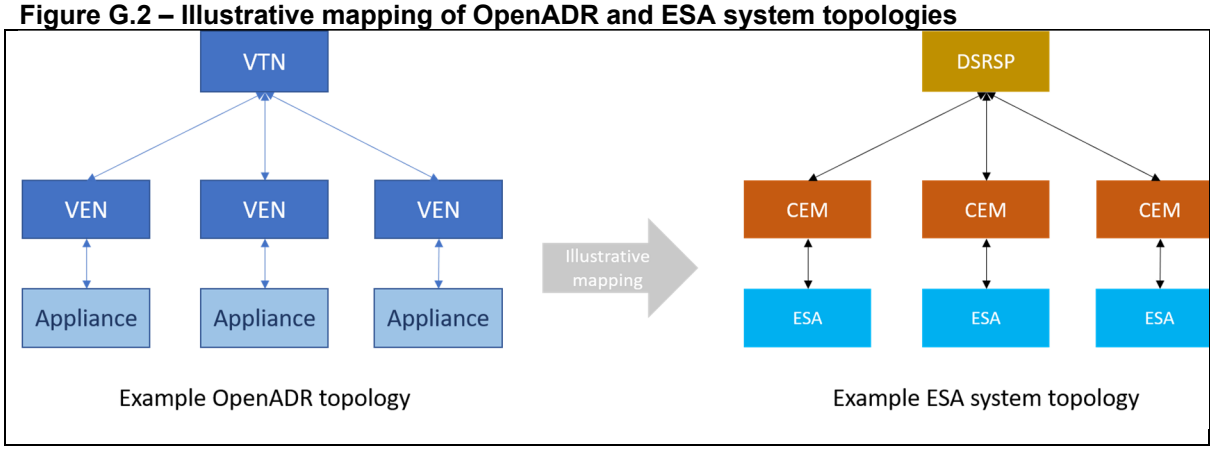


Figure G.2 – Illustrative mapping of OpenADR and ESA system topologies



Within the context of the ESA architecture defined in this PAS, the DSRSP takes the role of a VTN and the CEM takes the role of a VEN. The CEM/ESA interface is out of scope for OpenADR, although OpenADR is known to work with candidate protocols such as OCPP and the Energy Flexibility Interface (EFI, the basis for CLC TC205 EN50491-12-1).

G.4 Compatible communication protocols

The OpenADR system sits above the protocol stack and interfaces to OSI Application Layer (Layer 7). Two application layer protocols are supported, with slightly different characteristics:

- Hypertext Transfer Protocol (HTTP) – two modes are supported;
  - “pull mode” in which the CEN pulls information from the VTN. A poll message (oadrPoll) may be sent by the VEN to the VTN in order to request information from the VTN;
  - “push mode” in which the VTN is able to use “simple HTTP” (HTTP Push) to send messages to the VEN;
- Extensible Messaging and Present Protocol (XMPP) – bidirectional persistent connection.

It is likely that the DSRSP will send asynchronous requests to the CEM during normal operation. This should be supported by both the HTTP push and XMPP models.

G.5 Security

OpenADR includes cyber security measures that have been through NIST, SGIP and IEC Cyber-security reviews. The key points:

- server (VTN) and client (VEN) certificates are used;
- TLS1.2 is required for OpenADR certification (of products);
- DigiCert is used as the certification authority; and
- XML security wrappers are optional.

G.6 Transferring messages – OpenADR Services

There are four message categories, or service types, in OpenADR:

- Event (EiEvent Service) (NB: [1] includes the “full” EiEvent Service specification);
- Report (EiReport Service);
- Registration (EiRegisterParty Service); and
- Optional (EiOpt Service).

These Services are defined in detail in IEC 62746-10-1:2018 and are summarized here.

- The Event service is used by the VTN to send “command” types messages to the VEN.
- The Report service is used by the VEN to send “status” and “information” type messages to the VTN; basic initialization information.
- The Registration service is used whenever a VEN and a VTN first join and interact.
- The Optional service is used by the VEN to communicate short term status changes to the VTN.

The services map to the PAS 1878 Interface A messaging scheme in the following way:

- discovery, registration and initialization of the DSRSP and CEM/ESA partially map to the Registration service (the support of two phase authentication requires clarification);
- ESA flexibility offer selection messages, status update requests from the DSRSP to the CEM/ESA map to the Event service;
- flexibility offers, status updates, power values from the ESA/CEM to the DSRSP partially map to the Report service (the construction of profiles with different duration time slots requires clarification);
- the Optional service may not be required as flexibility offer updates will likely provide the equivalent functionality.

G.7 OpenADR messaging over Interface A

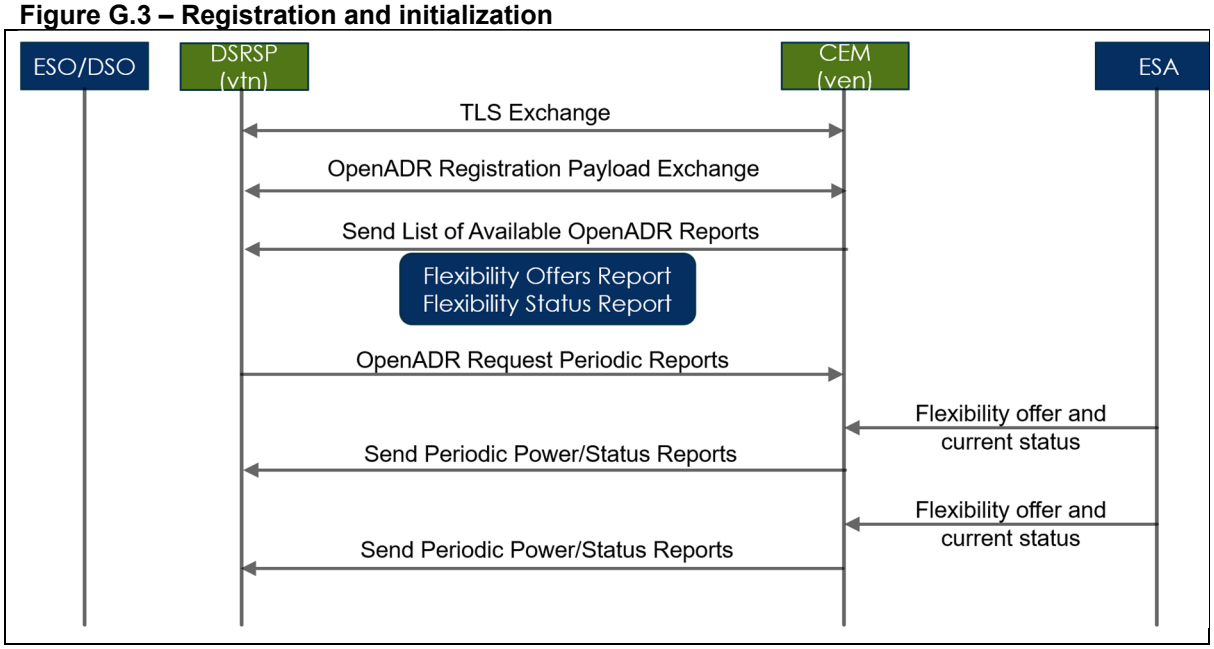
The message flows presented below map to those described in the draft PAS 1878.

G.7.1 Registration and initialization

The registration and initialization process is depicted in Figure G.3.

- The CEM is acting as the VEN, the DSRSP is acting as the VTN.
- Registration begins by setting up a secure connection using TLS (Note that two stage authentication requires clarification)
- Initialisation and capability negotiation using the OpenADR Registration service.
    - The CEM sends a oadrCreatePartyRegistration request to the VTN (this is used at first registration and for re-registration) including
        - Transport protocol (HTTP, XMPP)
        - Push support
    - The DSRSP responds with an oadrCreatedPartyRegistration payload, including
        - Identifiers for CEM and for DSRAP, for inclusion in payloads by the CEM
        - Profiles supported
        - Polling frequency (if CEM pull mode and polling is used)
- The CEM then sends a list of what type of reporting is available to the DSRSP – this includes flexibility offers such as power profiles.
- The DSRSP requests the CEM to begin sending reports (which may be sent asynchronously).
- The CEM sends status information and/or flexibility offer updates to the DSRSP whenever they are received from the ESA.

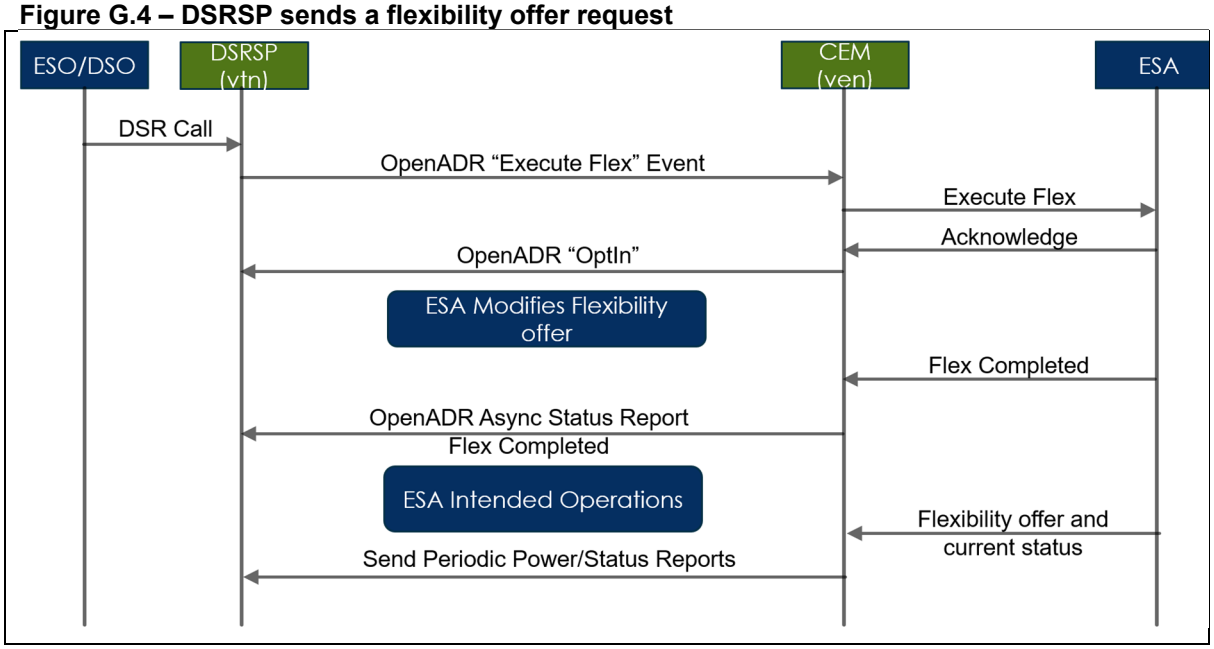
Figure G.3 – Registration and initialization



G.7.2 Flexibility offer request

- When the DSRSP receives a call from the ESO/DSO/DNO, it selects one of the available flexibility offers from each of its ESAs, via the CEM, using the OpenADR Event service.
- The acceptance of this request is acknowledged using OpenADR “Optin”.
- The ESA may update its flexibility offers at any time, thus triggering the CEM to send update reports to the DSRSP
- The ESA may be required to provide periodic actual power consumption figures during the period of the DSR event. The CEM passes this information to the DSRSP using the OpenADR Report service.
- Once the DSR event has been completed, the CEM informs the DSRSP using the Report service and the ESA/CEM return to sending updated flexibility and status reports to the DSRSP as required.

Figure G.4 – DSRSP sends a flexibility offer request



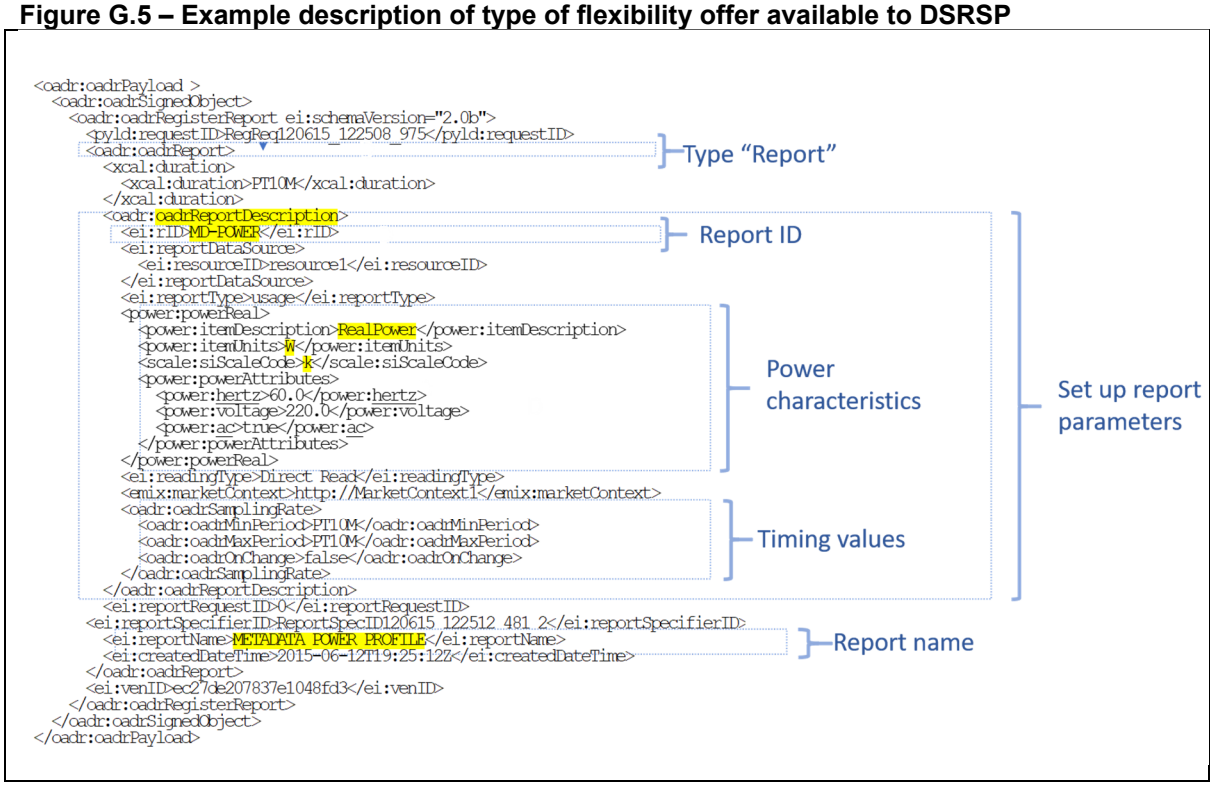
G.7.3 Structure of XML messages

This section described the structure of examples of the main messages in the above exchanges.

G.7.3.1 List of available flexibility offers supported

The XML for an example flexibility offer is shown in Figure **G.5**.

Figure G.5 – Example description of type of flexibility offer available to DSRSP



The main elements to note are:

- type “report” – this is an OpenADR EiReport Service message;
- report ID – the identifier (name) of the type of report;
- power characteristics – properties of power values reported including units (Watt), scaling (10^3 or kilo), line frequency (60Hz) and line voltage (220V);
- timing values – sampling values every 10 minutes; and
- report name – the name of the information included in the report.

G.7.3.2 Request from DSRSP to provide a particular flexibility offer report type

The XML for an example flexibility offer report type is shown in Figure **G.6**.

Figure G.6 – Request for example flexibility offer report type

```
<oadr:oadrPayload>
  <oadr:oadrSignedObject>
    <oadr:oadrCreateReport ei:schemaVersion="2.0b">
      <pyld:requestID>ReportReqID130615_192625_230</pyld:requestID>
      <oadr:oadrReportRequest>
        <ei:reportRequestID>ReportReqID130615_192625_730</ei:reportRequestID>
        <ei:reportSpecifier>
        <ei:reportSpecifierID>ReportSpecID1206</ei:reportSpecifierID>
          <xcal:granularity>
            <xcal:duration>PT10M</xcal:duration>
          </xcal:granularity>
          <ei:reportBackDuration>
            <xcal:duration>PT60M</xcal:duration>
          </ei:reportBackDuration>
          <ei:reportInterval>
            <xcal:properties>
              <xcal:dtstart>
                <xcal:date-time>2015-06-14T13:00:00Z</xcal:date-time>
              </xcal:dtstart>
              <xcal:duration>
                <xcal:duration>PT0M</xcal:duration>
              </xcal:duration>
            </xcal:properties>
          </ei:reportInterval>
          <ei:specifierPayload>
            <ei:rID>MD-POWER</ei:rID>
            <ei:readingType>x-notApplicable</ei:readingType>
          </ei:specifierPayload>
        </ei:reportSpecifier>
      </oadr:oadrReportRequest>
      <ei:venID>VEN130615_192312_582</ei:venID>
    </oadr:oadrCreateReport>
  </oadr:oadrSignedObject>
</oadr:oadrPayload>
```

Timing and duration values

Type of report requested

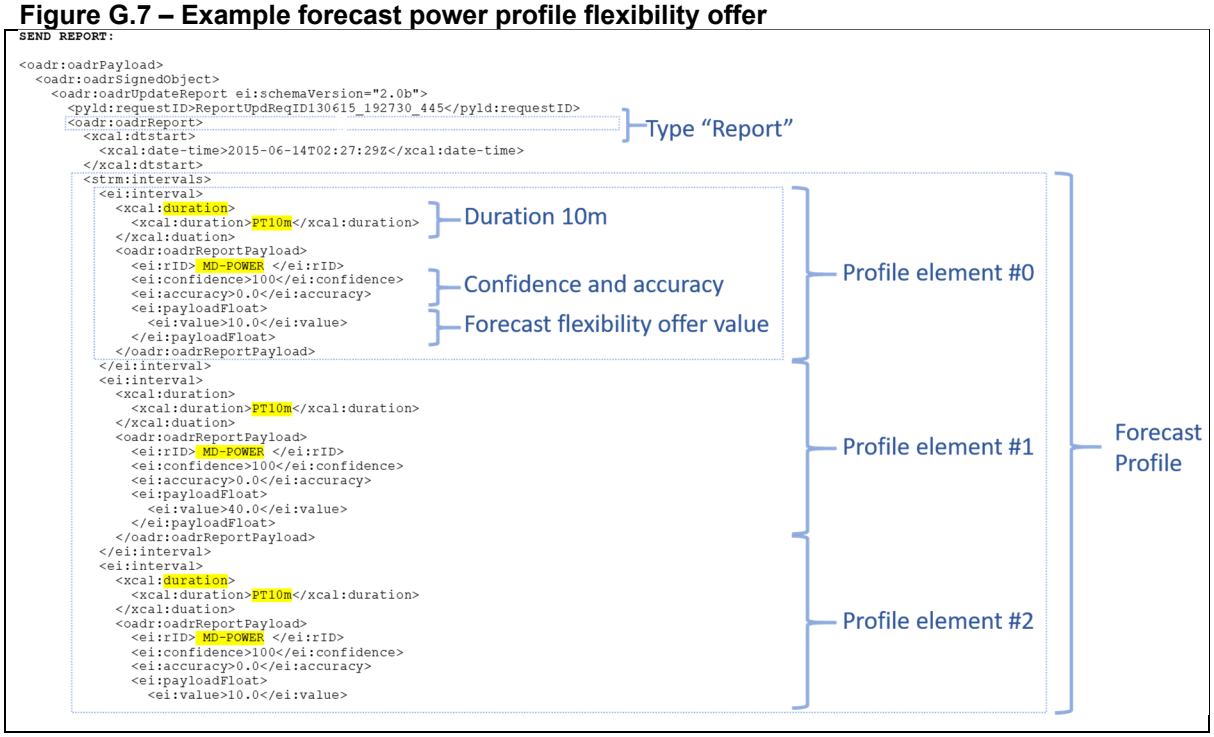
The main elements to note are:

- timing and duration values – timing granularity (10 minutes), duration of reporting period (60 minutes), start time of reporting period (13:00 on 14 June 2015); and
- type of report requested – the DSRSP may not require all possible report types.

G.7.3.3 Flexibility offer

The XML for an example forecast power profile flexibility offer from the ESA is shown in Figure G.7. Note that periodic power reports would likely be similarly constructed.

Figure G.7 – Example forecast power profile flexibility offer



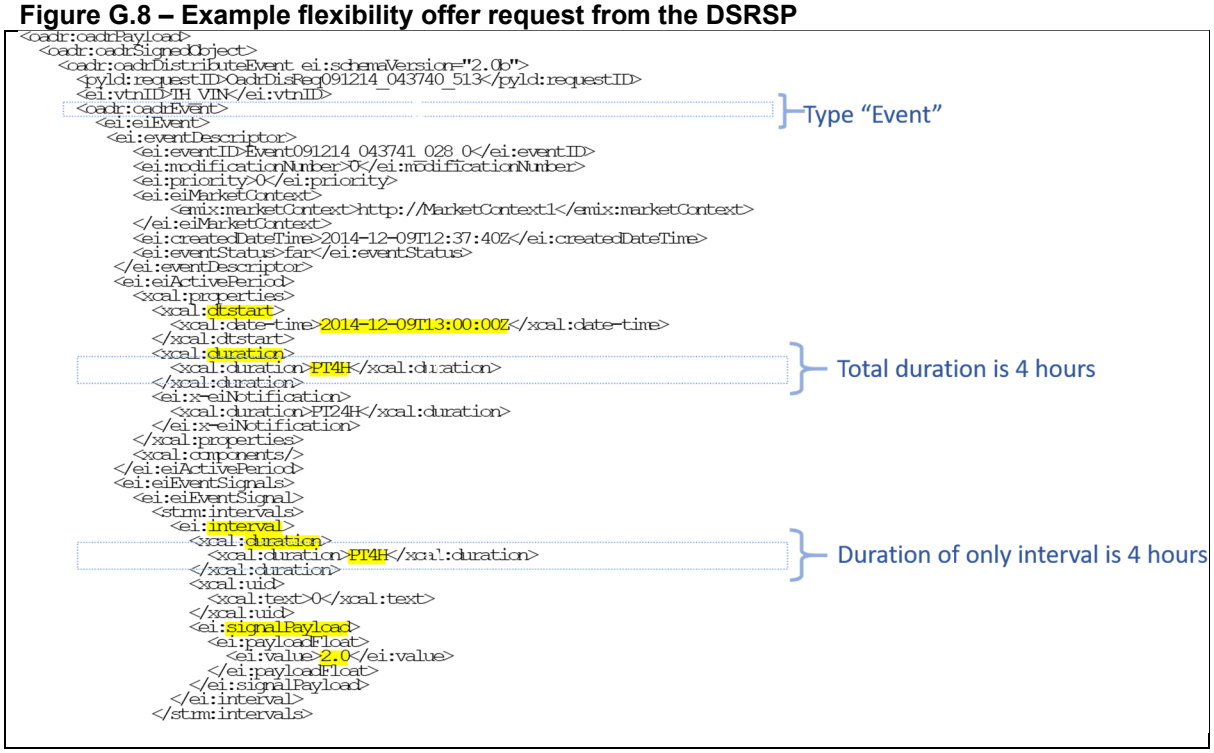
The main elements to note are:

- the main part of this report contains a series of profile “intervals”, each containing timing, confidence and accuracy values in addition to the forecast power value itself. Each “interval” is equivalent to a profile element; and
- the set of intervals constitutes the forecast power profile values.

G.7.3.4 Select flexibility offer

The XML for an example flexibility offer request message (eiEvent) from the DSRSP is shown in Figure G.8.

Figure G.8 – Example flexibility offer request from the DSRSP



The main elements to note are:

- this is an “event” message type;
- the total duration of the request is set to 4 hours;
- the duration of the only interval is 4 hours (as sum of interval durations must equal total duration)

G.8 Compatibility with PAS requirements

Below is a summary of the mapping of the high level requirements from the PAS on to the capabilities of OpenADR. Please note that this mapping is a first approximation and may be subject to re-evaluation.

G.8.1 Authentication

OpenADR supports TLS based authentication. Both the VTN (DSRSP) and VEN (CEM) are required to have certificates. Hence TLS based mutual authentication is performed.
The ability to use a second authentication stage with OpenADR is for further clarification.

G.8.2 Initialization

Table G.1 – Mapping of PAS 1878 initialization information requirements with possible OpenADR capabilities

Information element	Compatibility	Note
Flexibility offer types supported	Yes	Could be included as a report listed in oadrRegisteredReport metadata report
Power consumption report type supported	Yes	Could be included as a report listed in oadrRegisteredReport metadata report
Authentication	Yes	Could be included as a report listed in oadrRegisteredReport metadata report
ESA type	Maybe	Could be included as a report listed in oadrRegisteredReport metadata report
ESA classification	Maybe	Could be included as a report listed in oadrRegisteredReport metadata report

G.8.3 Normal operation

Table G.2 – Mapping of PAS 1878 normal operation (CEM/ESA to DSRSP) information requirements with possible OpenADR capabilities

Information element	Compatibility	Note
Flexibility offers	Likely yes	Could be defined as a report type. Clarification required on non-uniform profile element time series

Table G.2 – Mapping of PAS 1878 normal operation (CEM/ESA to DSRSP) information requirements with possible OpenADR capabilities

Information element	Compatibility	Note
Final power profile	Yes	Could be defined as a report type
Actual instantaneous power value	Yes	Could use existing Telemetry report type
Acknowledgements	Yes	Could be implemented using various specific acknowledgement messages
DSR event cancelled	Yes	Could be implemented as an updated flexibility offer or using oadrCancelOpt

Table G.3 – Mapping of PAS 1878 normal operation (DSRSP to CEM/ESA) information requirements with possible OpenADR capabilities

Information element	Compatibility	Note
Flexibility offer select (request)	Yes	Could be defined as an Eventvtype
DSR event cancelled	Yes	Could be implemented with specific message
Tariff	Yes	Could be implemented using EIQuote

G.8.4 Communications

OpenADR supports HTTP, simpleHTTP (for push mode) and XMPP. The ability to support push mode using simpleHTTP implies that the VTN (DSRSP) is able to send messages to the VEN (CEM) at any time rather than waiting to be polled by the VEN (CEM). This conforms to the DSRSP asynchronous messaging requirements of this PAS.

G.8.5 Information/data model

OpenADR is able to meet the majority of information model requirements of this PAS. There is some clarification required around the construction of the “profile” element. Profiles defined with elements of the same duration are supported in the existing schema. Profiles defined with elements of different durations may require to be represented as a series of single measurements.
XML is used to describe the data model over the wire. There are currently no JSON implementations.

G.9 Conclusion

OpenADR was developed to allow straightforward transactional communication between grid and end point entities. It provides a communications framework and a data model schema. Although the system could be used to reach as far as an ESA, a gateway is generally used between OpenADR on the grid-side and the ESA in the home-side.
The OpenADR ecosystem is mature and generally well developed. There tends to be a focus on North America, Japan, Korea and China. There is now increased activity in the European Region.
Security makes use of TLS and supports mutual authentication, key management would be expected to be in line with existing guidelines. OpenADR 2.0 is compliant with with NIST Smart Grid security guidelines etc. A single Certification Authority has been assigned for use with OpenADR product.

Certification is readily available in North America and East Asia. It seems that there are no test houses in Europe at the moment, although this may change over time (for instance, a German university is offering test facilities in their laboratories in South Korea).
OpenADR 2.0b came out of the OASIS Interoperable Energy specification 1.0 and has been standardized by the IEC. An OpenADR/CIM mapping specification has also been standardized. There appear to be no plans for further standardization at IEC level.
OpenADR is a suitable candidate for further investigation into its ability to satisfy the requirements of this PAS.

Annex H (informative)
EEBus

COMMENTARY ON ANNEX H

This Annex provides an overview of the EEBus ecosystem and technical specifications. It is entirely informative and attempts to provide information on a best effort basis. Examples are provided for illustrative purposes only. The reader should return to the references for any definitive information.

H.1 Specifications and standardization

The EEBus data model, message flow and application layer was standardized by CENELEC as BS EN 50631-1 *Household appliances network and grid connectivity – Part 1: General Requirements, Generic Data Modelling and Neutral Messages*. This followed on from a Technical Report on smart grid and smart appliance use cases, IEC TR 62746-2 *Systems interface between customer energy management system and the power management system – Part 2: Use cases and requirements* from a joint working group involving CENELEC and IEC smart grid related Technical Committees (CENELEC TC59X (the smart appliance), CENELEC TC205 (S2 Interface and the CEM) and IEC TC57 (grid-side actors)).

NOTE A new version of BS EN 50631-1 is planned for the end of 2020, along with the production of new standards in the series:

- EN 50631-1 Ed 2 *General Requirements, Generic Data Modelling and Neutral Messages* will be a slimmed down version of the original and will focus on generic requirements and Use Case Functions (high level building blocks and a key part of the 50631-1 approach). It will no longer contain the SHIP (Smart Home IP) specification [20].
- EN 50631-2 *Product Specific mappings, details, requirements and deviations* will be a mapping of typical features onto particular product categories.
- EN 50631-3-x *Specific Data Model Mapping* will be a set of three documents mapping Use Case Functions onto specific existing data model/protocols, such as SPINE (Smart Premises Interoperable Neutral-Message Exchange) and Echonet-lite.
    - EN 50631-3-1 will the mapping of the Use Case Functions onto SPINE.
- EN 50631-4-1 *Communication Protocol Specific Aspects* will be the SHIP protocol specification. Other transport protocols will be covered in other sub-parts, possibly including IEC 61850 series.
- EN 50631-5 *General Test-Requirements & Specifications* will be a test requirement specification.
- EN 50631-6 *SPINE Data Model Toolbox* will be the detailed SPINE specification.

All new documents will apply to white goods and to HVAC systems.

CENELEC TC59X, which developed EN 50631-1) and CENELEC TC205 (which developed BS EN 50491-12-1:2018) have been working closely together since 2012. Coordinated activities have included developing IEC TR 62746-2:2015 and in collaborating on the input for other projects such as the European Commission *Study on ensuring interoperability for enabling Demand Side Flexibility* [17].

In general, EN 50631-1 fits well into the smart grid flexibility landscape being developed in European and International standards bodies. It has a clear mapping to the Smart Grid Architecture Model (SGAM) and is 100% compatible with SAREF (Smart Appliance Reference Ontology) and SAREF4ENER (a SAREF extension for energy systems) embodied in ETSI standards ETSI TS 103 264 V1.1.1 SmartM2M; "*Smart Appliances; Reference Ontology and oneM2M Mapping*" [18] and ETSI TS 103 410-1 V1.1.1 SmartM2M; "*Smart Appliances Extension to SAREF; Part 1: Energy Domain*" [19] (SAREF4ENER is based upon EEBus).

EEBus originally focused on the smart appliance communications interface and functionality. Recently, it has been working on smart EV charging systems and now also looking at the interface between the premises boundary and the CEM for smart grid applications. Standardization work in these areas is ongoing at a national level in Germany.

NOTE EEBus specifications and additional information are available from the EEBus Intiative website[1)].

H.2 Take-up and ecosystem

Strategy development, promotion and technical development of EEBus is managed by the EEBus Initiative. EEBus is primarily a German organization although membership includes many companies including large international corporations in the appliance, EV, equipment, utility, research and communications sectors. Board members include Bosch, Hager, Miele, Vaillant and a previous CENELEC President. Members include IBM, Daikin, SMA, E-on, Schneider Electric, Deutsche Telekom and Microsoft. The EEBus Initiative has links with other organizations such as IBM Watson, Volkswagen-Audio, Open Charge Alliance, Thread, Energy@Home and the Open Connectivity Foundation. EEBus is also involved in the EC JRC Smart Grid Interoperability Laboratory and is a member of the Interconnect Project (https://interconnectproject.eu/).

EEBus originally focused on the smart appliance communications interface and functionality. Recently, it has been working on smart EV charging systems and now also looking at the interface between the premises boundary and the CEM for smart grid applications; and cloud systems.

There are currently five Working Groups developing technical specifications to integrate their domains into an energy management system of a premises with or without an interface to the energy grid:

- E-mobility – charging stations, electric vehicles
  - Including Volkswagen-Audi, BMW
- HVAC – heating (HP), ventilation, air conditioning and cooling
  - Including Daikin, Vaillant, Bosch, Viessmann
- Inverter – PV and storage battery systems
- Grid – demand transparency and set points by DSO
- Commercial – energy domains in commercial buildings
- General participation from Whirlpool, Miele and Siemens

EEBus is used in the Audi e-tron for smart charging, in Bosch home appliances, Danfoss/SMA supermarket HVAC/refrigeration/photovoltaic/energy storage/EV charging solutions, SMA energy managers, Microsoft Azure, and the Enervalis Smartpower Suite.

There is currently no EEBus certification accreditation scheme, although clearly from the proposed new standards (EN 50631-5), testing and certification will become more visible in the near future. Several PlugFests have been held (including with Audi) and the UDE has a SPINE/SHIP test system that can provide a form of certification. Interoperability testing focuses on the minimum required functions only. EEBus is, however, working on a test system and test and developer tools are available from EEBus board member KEO.

Geographically, EEBus seems to be focused mostly within Europe.

H.3 System overview

The EEBus architecture includes the Smart Premises Interoperable Neutral-Message Exchange (SPINE) and Smart Home IP (SHIP) specifications. SPINE sits above SHIP in the protocol stack but is not dependent upon a SHIP implementation being present as it has

[1)] More information can be found at https://www.eebus.org/

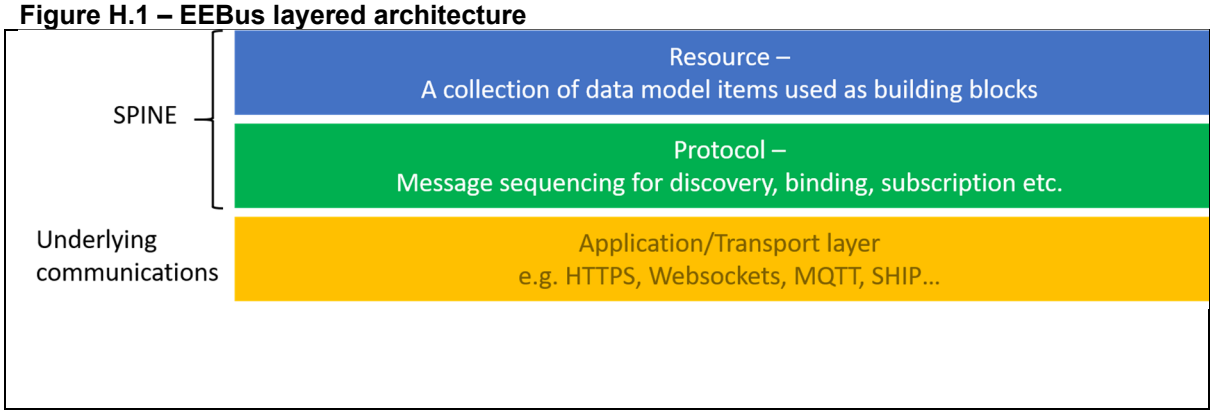
been designed to run over a number of application/transport layer protocols including HTTPS, Websockets and MQTT.

SPINE is itself divided into two sub-specifications, as shown in Figure H.1.

The Protocol specification includes aspects of message sequencing and associated information (equivalent to header information). This specification is used to describe how EEBus entities discover, address, bind, subscribe and so on.

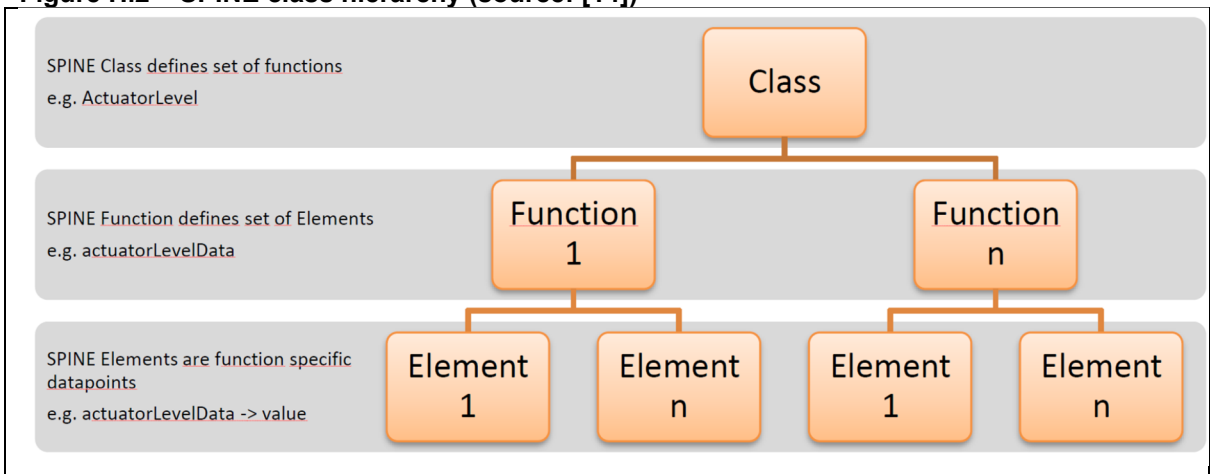
The Resource Specification includes collections of data structures and actions. These effectively form a tool box of available resource and may be used to satisfy a range of functions, device descriptions and/or use cases.

Figure H.1 – EEBus layered architecture



SPINE resources form a hierarchy as shown in Figure H.2. In SPINE, functions are used to build up the capabilities required by a use case.

Figure H.2 – SPINE class hierarchy (source: [14])



SOURCE: EEBus SPINE Technical Report – Introduction v1.1.1, EEBus Initiative, 2018

Functions are described using .XSD format but “over the wire” implementation is not limited to XML. JSON implementations are available.

SPINE defines many functions, most of which will not be required for the minimum functionality requirements of this PAS. Some functions and elements of SPINE are mandatory but many of them are optional, allowing a reduced footprint version of EEBus to be used if desired.

H.4 Compatible communication protocols

SPINE is able to run over SHIP, HTTP(S), Secure Websockets (over TLS/TCP) and MQTT.

DNS Service Discovery (DNS-SD - RFC 6763) is used for EEBus device/service discovery and Multicast DNS (mDNS – RFC 6762) is used over UDP to send network setup message to all EEBus participants. Both may be used over UDP.

EEBus is designed to run over UDP/TCP and Internet Protocol (IP).

H.5 Security

SHIP mandates the use of Websockets (RFC 6455) over TLS 1.2 mutual authentication between all SHIP nodes. The use of Websockets allows a connection between EEBus nodes to remain open for full duplex communication.

Key management procedures, including Subject Key Identifier (SKI), SHIP node PIN and QR code, are defined in the SHIP specification.

Two-factor authentication is possible using SHIP, which also supports three different user interaction modes (above the same TLS implementation) for different levels of device sophistication and customer knowledge.

Pending further scrutiny, it seems that EEBus cyber-security capabilities are likely to meet the high level cyber-security requirements of this PAS.

H.6 EEBus messaging over Interface A

This section uses diagrams from EEBus to demonstrate how existing and newly proposed EEBus UC functions (UCF) can be used to transfer flexibility offers, power values and status.

H.6.1 ESA/CEM registration with DSRSP

SHIP defines the registration with secure verification processes between an

The message sequence chart for this operation in shown in Figure H.3 and the information content in Figure H.4. This includes capability information exchange and addressing.

Note that the information content is divided into three sets, corresponding to the EEBus concept of “device”, “entity” and “feature”. The “address” fields in each are dependent upon the underlying protocol and so are populated accordingly.

Figure H.3 – CEM registers with DSRSP

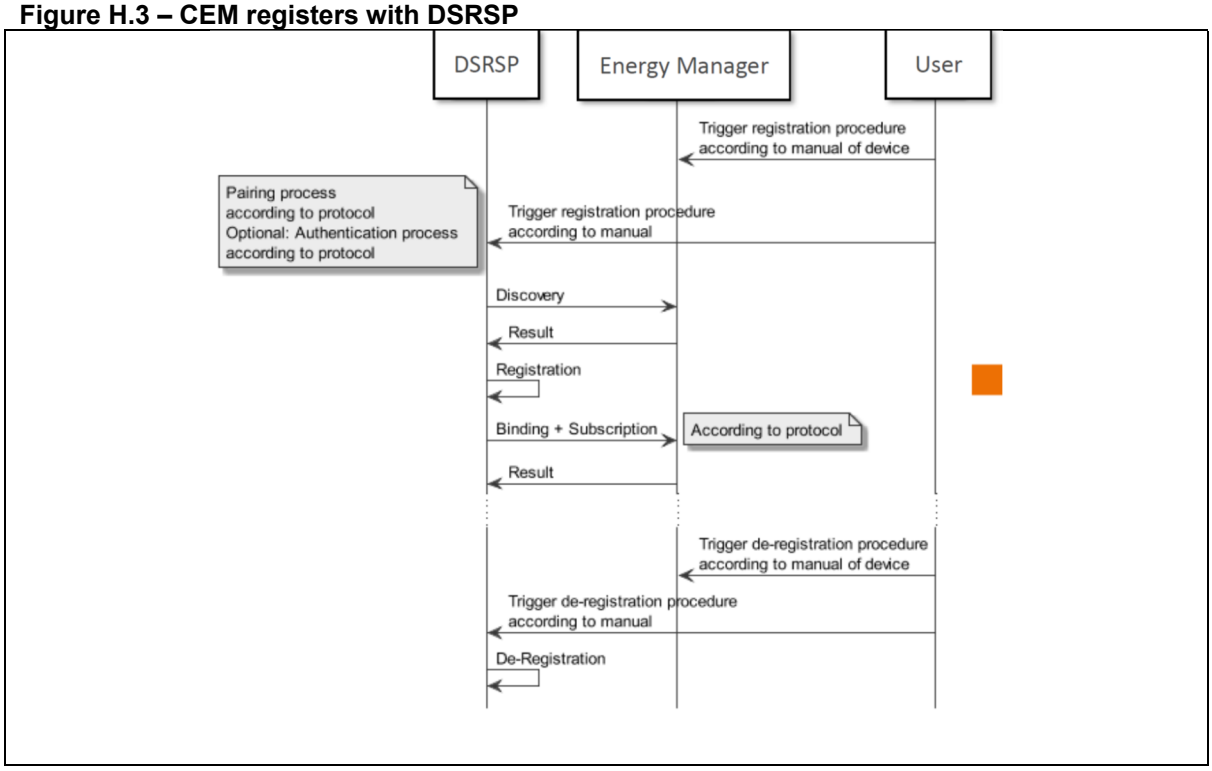
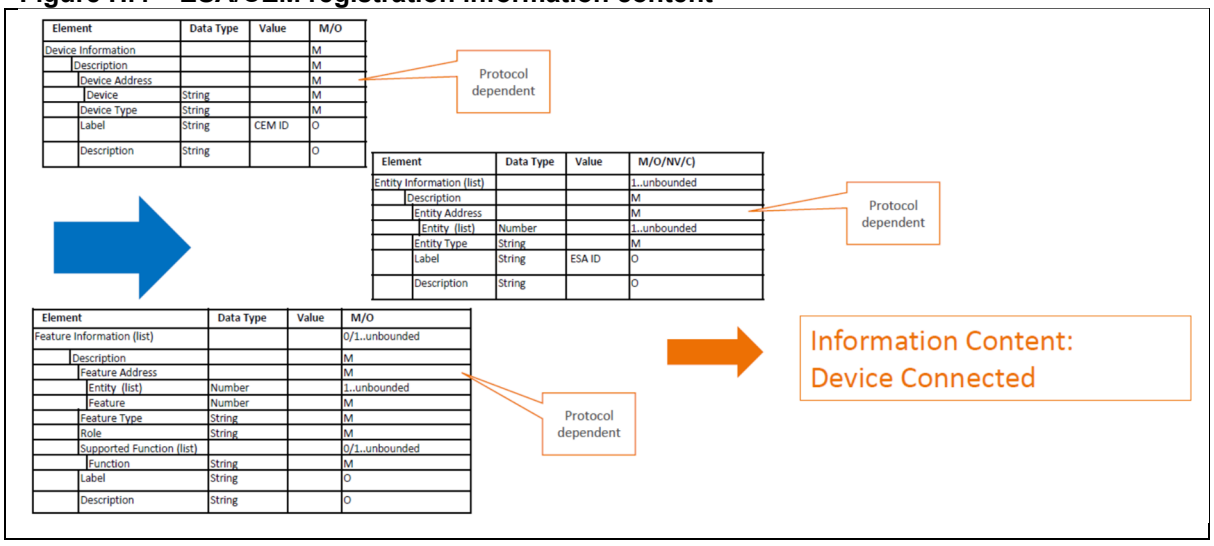


Figure H.4 – ESA/CEM registration information content



This functionality is provided by the “EEBus_SPINE_TS_NodeManagement” function. The SPINE message flow is show in Figure H.5 and the XML datagram for the first message, nodeManagementSubscriptionRequestCall, is shown in Figure H.6.

Figure H.5 – UCF_Device_Connected SPINE message flow

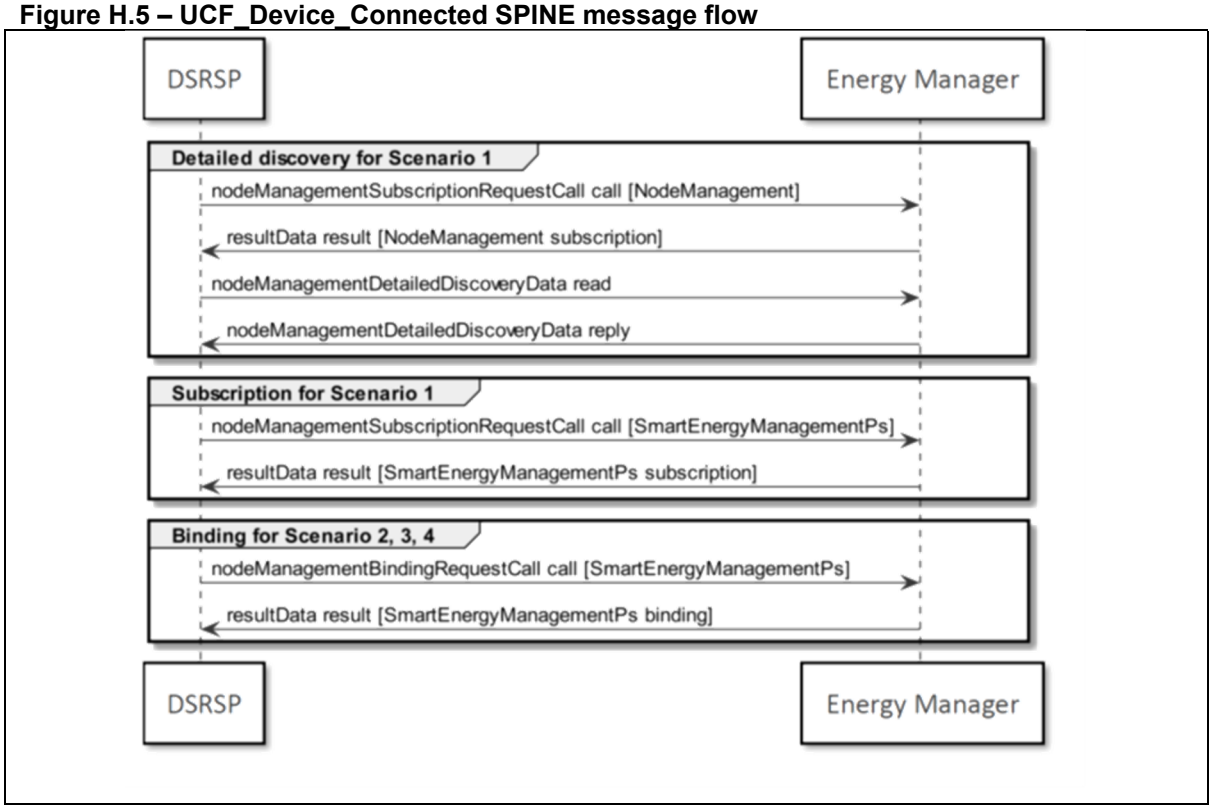


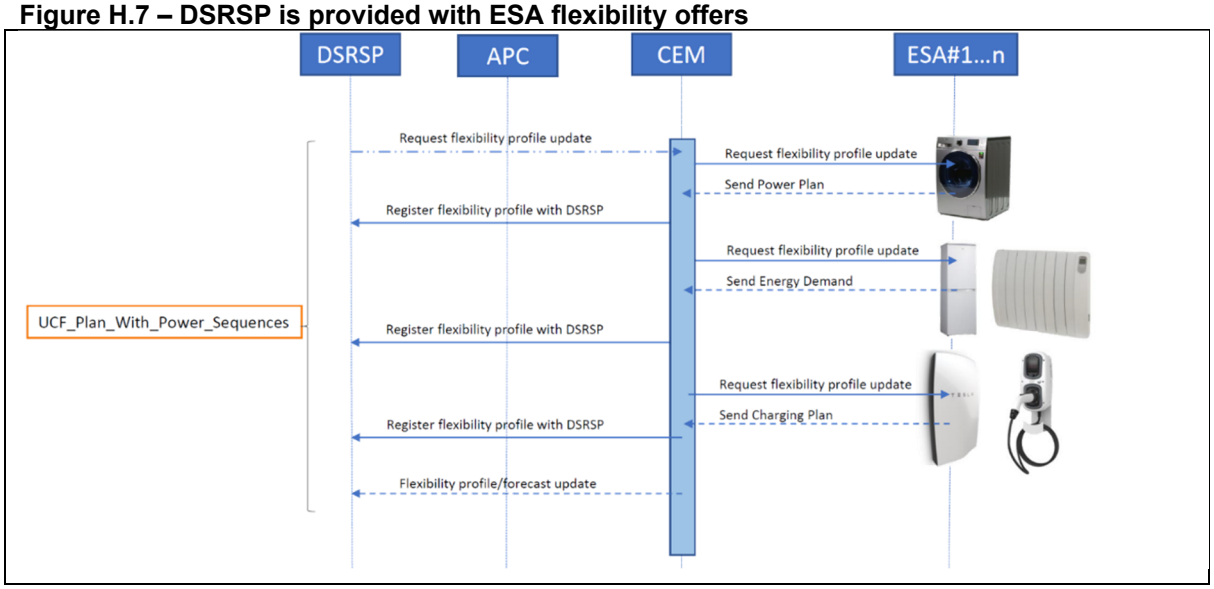
Figure H.6 – UCF_Device_Connected first message datagram

Some EEBus registration process features seem suitable for use by this PAS and further clarification is required.

H.6.2 ESA provides flexibility offers to DSRSP via CEM

The message sequence chart for this operation is shown in Figure H.7, where three ESAs are providing their flexibility offers to the DSRSP. This figure also shows how a use case function (UCF) can be built up from functions (building blocks).

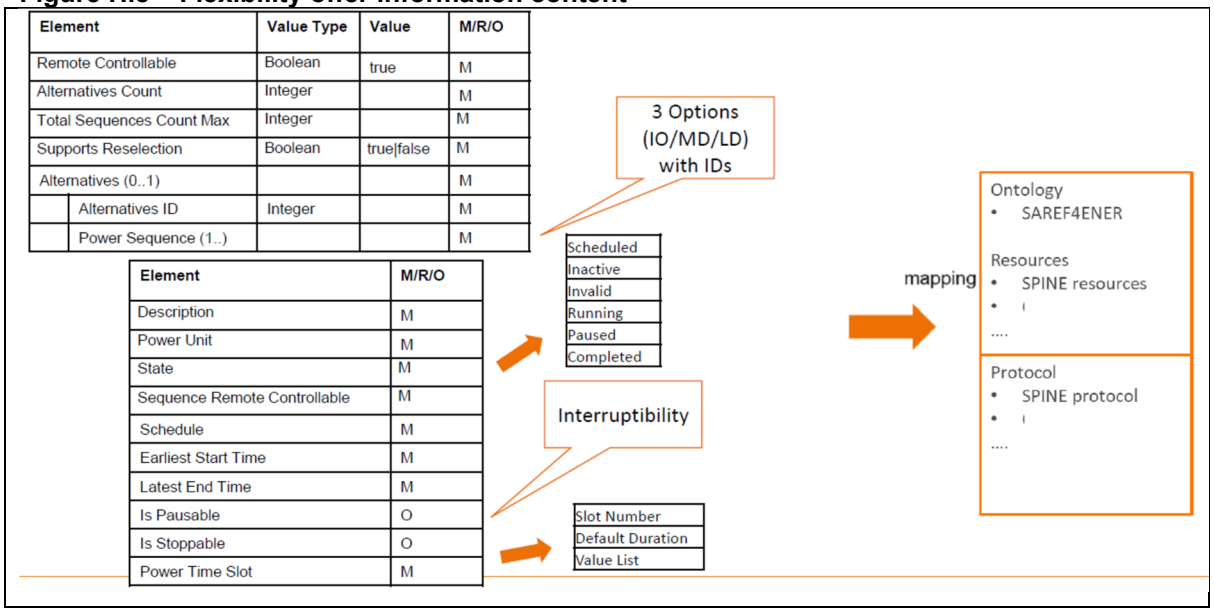
Figure H.7 – DSRSP is provided with ESA flexibility offers



More detail on the information content of the flexibility offering is shown in Figure H.8. This includes forecast profiles (LD/IO/MD), scheduling information and whether or not a power slot (a constituent of a sequence) is able to be paused or stopped.

This functionality is provided by the “EEBus_SPINE_TS_SmartEnergyManagementPs” and “EEBus_SPINE_TS_PowerSequences” functions.

Figure H.8 – Flexibility offer information content



The SPINE dataflow is shown in Figure H.9, the XML payload of the SmartEnergyManagementPs message is shown in Figure H.10 and the whole SmartEnergyManagementPs message JSON datagram is show in Figure H.11.

Figure H.9 – TS_SmartEnergyManagementPs SPINE message flow

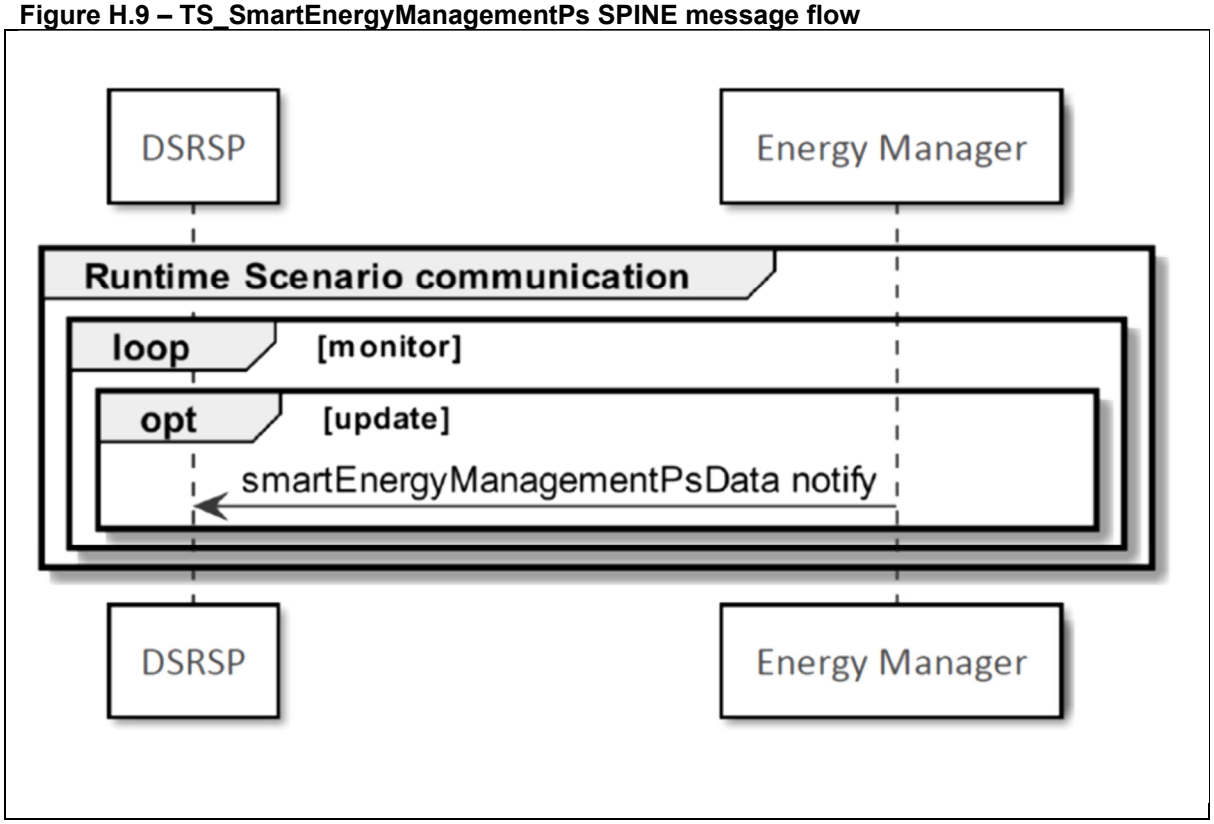


Figure H.10 – TS_SmartEnergyManagementPs SPINE message XML payload

```
<payload>
    <cmd>
      <smartEnergyManagementPsData>
        <nodeScheduleInformation>
          <nodeRemoteControllable>true</nodeRemoteControllable>
          <supportsSingleSlotSchedulingOnly>true</supportsSingleSlotSchedulingOnly>
          <alternativesCount>1</alternativesCount>
          <totalSequencesCountMax>2</totalSequencesCountMax>
          <supportsReselection>true</supportsReselection>
        </nodeScheduleInformation>
        <alternatives>
          <relation>
            <alternativesId>1</alternativesId>
          </relation>
          <powerSequence>
            <description>
              <sequenceId>1</sequenceId>
              <powerUnit>W</powerUnit>
              <valueSource>calculatedValue</valueSource>
            </description>
            <state>
              <state>scheduled</state>
              <sequenceRemoteControllable>true</sequenceRemoteControllable>
            </state>
            <schedule>
              <startTime>PT1H7M</startTime>
              <endTime>PT2H9M</endTime>
            </schedule>
            <scheduleConstraints>
              <earliestStartTime>PT0S</earliestStartTime>
              <latestEndTime>PT11H23M</latestEndTime>
            </scheduleConstraints>
            <powerTimeSlot>
              <schedule>
                <slotNumber>1</slotNumber>
                <defaultDuration>PT1H2M</defaultDuration>
              </schedule>
              <valueList>
                <value>
                  <valueType>powerExpectedValue</valueType>
                  <value>
                    <number>1200</number>
                    <scale>0</scale>
                  </value>
                </value>
              </valueList>
            </powerTimeSlot>
          </powerSequence>
        </alternatives>
      </smartEnergyManagementPsData>
    </cmd>
  </payload>
</datagram>
```

1st alternative = flexibility offer identifier

Power sequence start

Units in Watts

Schedule start/end times

Start/end time constraints

1 of 1 slot

Slot duration 1 hour 2 mins

Expected power1200 Watts

Figure H.11 – TS_SmartEnergyManagementPs SPINE message JSON datagram


```
{"datagram": [
        {"header": [
                {"specificationVersion": "1.1.0"}, {"addressSource": [{"device": "d:_i:46925_EnergyManager"}, {"entity": [1]},
                {"feature": 1}]}, {"addressDestination": [{"device": "d:_i:46925_DSRSP"}, {"entity": [1]}, {"feature": 1}]},
                {"msgCounter": 200}, {"msgCounterReference": 100}, {"cmdClassifier": "reply"}, {"ackRequest": true},
                {"timestamp": "2019-09-13T16:00:20.0Z"}]},
        {"payload": [
                {"cmd": [{
                        {"smartEnergyManagementPsData": [
                                {"nodeScheduleInformation": [
                                        {"nodeRemoteControllable": true},
                                        {"supportsSingleSlotSchedulingOnly": true},
                                        {"alternativesCount": 1},
                                        {"totalSequencesCountMax": 2},
                                        {"supportsReselection": true}]},
                                {"alternatives": [{
                                        {"relation": [
                                                {"alternativesId": 1}]},
                                        {"powerSequence": [{
                                                {"description": [
                                                        {"sequenceId": 1},
                                                        {"powerUnit": "W"},
                                                        {"valueSource": "calculatedValue"}]},
                                                {"state": [
                                                        {"state": "scheduled"},
                                                        {"sequenceRemoteControllable": true}]},
                                                {"schedule": [
                                                        {"startTime": "PT1H7M"},
                                                        {"endTime": "PT2H9M"}]},
                                                {"scheduleConstraints": [
                                                        {"earliestStartTime": "PT0S"},
                                                        {"latestEndTime": "PT11H23M"}]},
                                                {"powerTimeSlot": [
                                                        {"schedule": [
                                                                {"slotNumber": 1},
                                                                {"defaultDuration": "PT1H2M"}]},
                                                        {"valueList": [
                                                                {"value": [
                                                                        {"valueType": "powerExpectedValue"},
                                                                        {"value": [
                                                                                {"number": 1200},
                                                                                {"scale": 0}]
                                                        }]}]}]}]}]}]}]}]}]}
```


1st alternative = flexibility offer identifier

Power sequence start

Units in Watts

Schedule start/end times

Start/end time constraints

1 of 1 slot

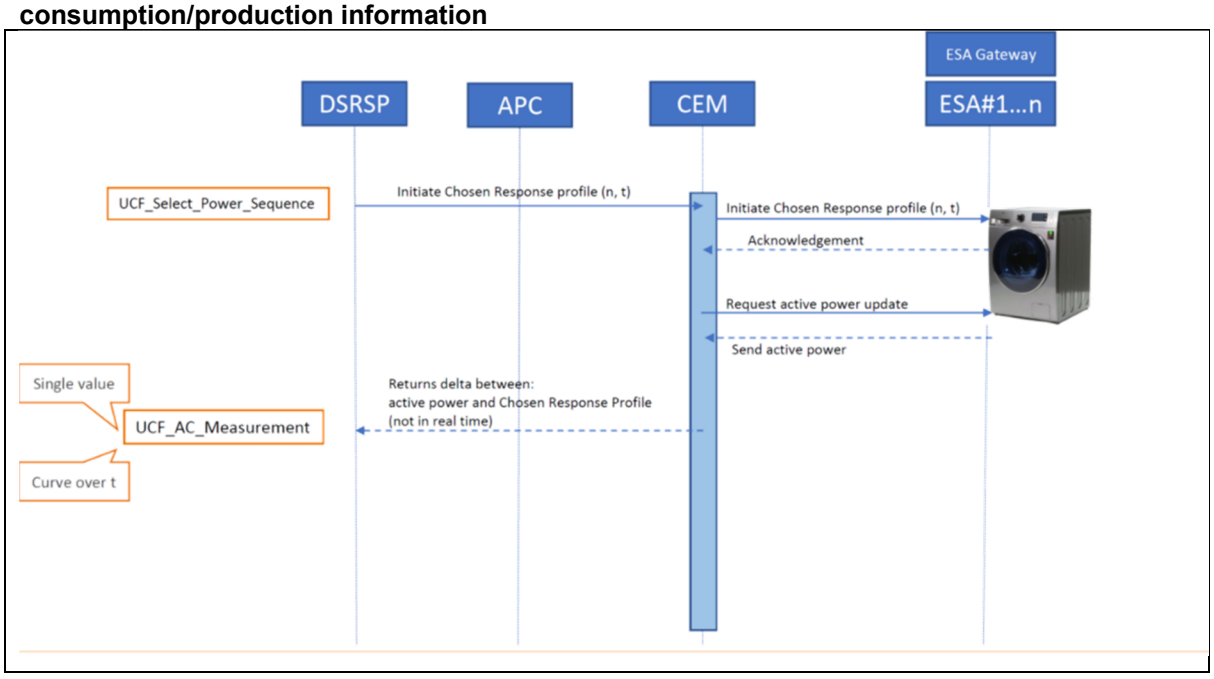
Slot duration 1 hour 2 mins

Expected power1200 Watts

H.6.3 DSRSP requests a flexibility offer and the ESA provides power consumption/production

The message sequence chart for this operation in shown in Figure H.12. Here the DSRSP selects one of the flexibility offers previously provided to it. The ESA provides either periodic power consumption/production values or a profile of values

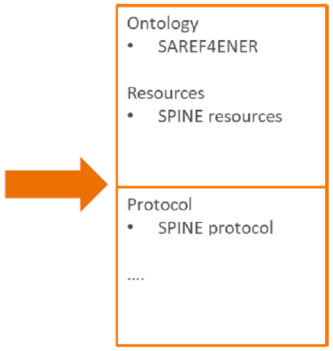
Figure H.12 – DSRSP requests flexibility offer and ESA provides power consumption/production information



The information content for the DSRSP request, including schedule information, is shown in Figure H.13.

Figure H.13 – DSRSP request information content

Element			Data Type	Value	M/R/O
Alternatives					M
	Power Sequence				M
		Sequence ID	Integer		M
		Schedule			M
		Start Time	Duration	<xs:duration>	M



The information content for the consumption/production power value is shown in Figure H.14. As much of this information is static in the PAS 1878 implementation, it may be possible to transfer only the information related to the dynamic portion.

Figure H.14 – Power consumption/production information content

Element	Data Type	Value		M/R/O
Measurement ID	Integer			M
Measurement Type	String	"power"	"energy"	M
Commodity Type	String	"electricity"	"electricity"	M
Unit	String	"W"	"Wh"	M
Scope Type	String	"acPower" "acPowerTotal"	"acEnergy"	M

Element	Data Type	Value	M/R/O
Measurement ID	Integer		M
Value Range Min	Number		R
Value Range Max	Number		R
Value Step Size	Number		R

Element	Data Type	Value	M/R/O
Measurement ID	Integer		M
Value Type	String	"value"	M
Timestamp	Duration or DateTime		O
Value	Number		M
Evaluation Period			O
Start Time	Duration or DateTime		M
End Time	Duration or DateTime		M
Value Source	String	„measuredValue“ „calculated Value“ „empiricalValue“	M
Value State	String	„normal“ „outOfRange“ „error“	R

Element	Data Type	Value	M/R/O
Electrical Connection ID	Integer		M
Power Supply Type	String	"ac"	M
Positive Energy Direction	String	„consume“	M

Element	Data Type	Value	M/R/O
Electrical Connection ID	Integer		M
Parameter ID	Integer		M
Measurement ID	Integer		M
Voltage Type	String	"ac"	M
AC Measurement Type	String	„real“	M

This functionality is provided by the “EEBus_SPINE_TS_SmartEnergyManagementPs” and “EEBus_SPINE_TS_Measurement” functions.

The SPINE dataflow is shown in Figure H.15, the XML payload of the SmartEnergyManagementPsData message is shown in Figure H.16 and the whole SmartEnergyManagementPsData message JSON datagram is show in Figure H.17.

Figure H.15 – TS_SmartEnergyManagementPsData SPINE message flow

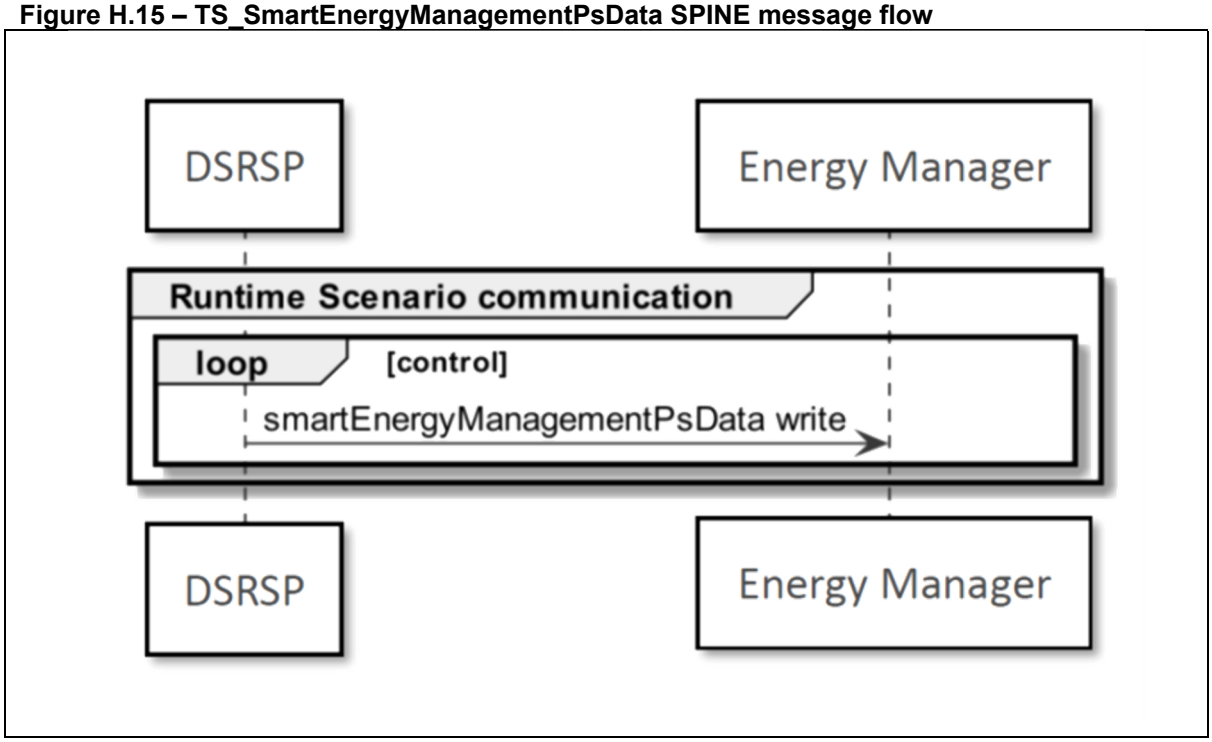
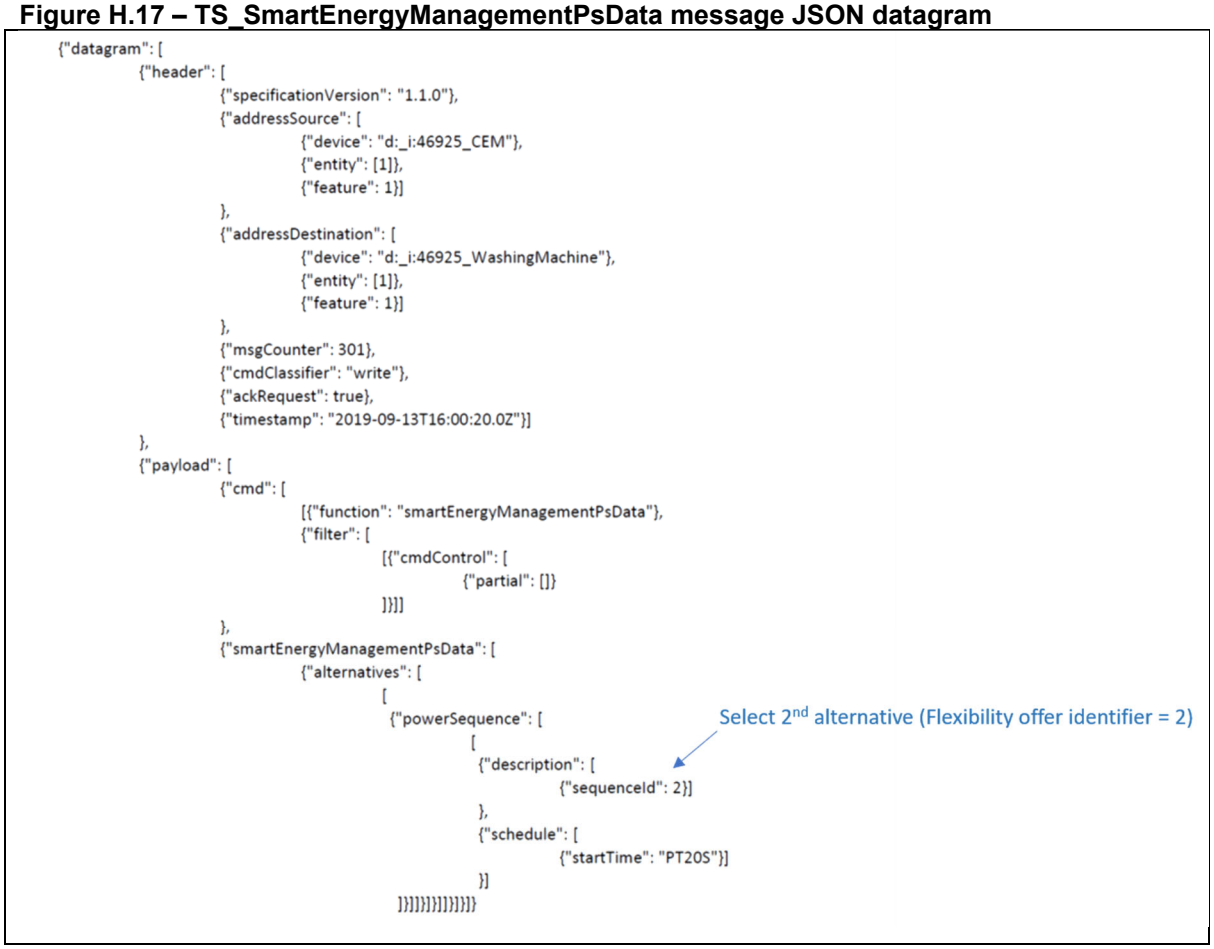


Figure H.16 – TS_SmartEnergyManagementPsData message XML payload

```
<payload>
    <cmd>
      <function>smartEnergyManagementPsData</function>
      <filter>
        <cmdControl>
          <partial/>
        </cmdControl>
      </filter>
      <smartEnergyManagementPsData>
        <alternatives>
          <powerSequence>
            <description>
              <sequenceId>2</sequenceId>
            </description>
            <schedule>
              <startTime>PT20S</startTime>
            </schedule>
          </powerSequence>
        </alternatives>
      </smartEnergyManagementPsData>
    </cmd>
  </payload>
</datagram>
```

Select 2nd alternative (Flexibility offer identifier = 2)

Figure H.17 – TS_SmartEnergyManagementPsData message JSON datagram



H.7 Compatibility with PAS requirements

This section summarizes the mapping of the high level requirements from the PAS on to the capabilities of EEBus. Please note that this mapping is a first approximation and may be subject to re-evaluation.

H.7.1 Authentication

EEBus requires TLS based mutual authentication. Two stage authentication is also possible. Three different customer interaction modes, running over TLS, are available. Discovery is performed using industry standard protocols (RFCs).

H.7.2 Initialization

Table H.1 – Mapping of PAS 1878 initialization information requirements with possible OpenADR capabilities

Information element	Compatibility	Note
Flexibility offer types supported	Yes	nodeManagementxx, JWG-F100
Power consumption report type supported	Yes	nodeManagementxx, JWG-F100
Authentication	Yes	Using SHIP (TLS)
ESA type	Maybe	nodeManagementxx, JWG-F100
ESA classification	Maybe	nodeManagementxx, JWG-F100)

H.7.3 Normal operation

Table H.2 – Mapping of PAS 1878 normal operation (CEM/ESA to DSRSP) information requirements with possible OpenADR capabilities

Information element	Compatibility	Note
Flexibility offers	Yes	SmartEnergyManagementPs
Final power profile	Yes	SmartEnergyManagementPs
Actual instantaneous power value	Yes	SmartEnergyManagementPs
Acknowledgements	Yes	Use of cmdClassifier
DSR event cancelled	Yes	SmartEnergyManagementPs

Table H.3 – Mapping of PAS 1878 normal operation (DSRSP to CEM/ESA) information requirements with possible OpenADR capabilities

Information element	Compatibility	Note
Flexibility offer select (request)	Yes	SmartEnergyManagementPs
DSR event cancelled	Yes	SmartEnergyManagementPs
Tariff	Yes	To be clarified

H.7.4 Communications

EEBus supports Websockets, TLS, MQTT and TCP over IP. mDNS and DNS-SD are used over UDP for device and service discovery.

This is in line with the requirements of this PAS.

H.7.5 Information/data model

EEBus uses a comprehensive data and message sequence model, SPINE. Investigations to date have not indicated any issues with the information content of the data model, although further clarification is required.

The data model is compatible with SAREF4ENER. This should greatly ease the translation between EEBus and other data models, as the SAREF4ENER ontology definitions can be used as a bridge or “dictionary”.

Both XML and JSON are supported natively.

H.8 Conclusion

EEBus originally focused on the interface specification between smart appliances and a communications manager (similar) to the CEM. The scope of work has now expanded to include EV charging stations, CEM to premises boundary (SGCP) and even into the grid (through work with DSOs on IEC 61850 interworking).

Although the EEBus ecosystem is still relatively undeveloped and tends to centre around Europe, membership includes several large companies and involvement with other organisations is high.

Security seems to be well thought out and would be expected to be in line with existing guidelines. Further clarification is required in order to ascertain alignment with NIST Smart Grid security guidelines etc.

Certification is relatively undeveloped, but there is movement in standards at least to define a test specification. Certification is currently possible using one test house and test tools are available.

SPINE (the data and messaging model) has been standardized in CENELEC and there is a clear plan for further standardization in order to extend and clarify standardization coverage, including an expansion of the application base to HVAC.

A suitable candidate for further investigation into its ability to satisfy the requirements of this PAS.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN 16836-1, *Communication systems for meter – Wireless mesh networking for meter data exchange – Part 1: Introduction and standardization framework*

BS EN 16836-2, *Communication systems for meter – Wireless mesh networking for meter data exchange – Part 2: Networking layer and stack specification*

BS EN 50491-12-1:2018, *General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Smart grid – Application specification – Interface and framework for customer – Interface between the CEM and Home/Building Resource manager – General Requirements and Architecture*

BS EN 50631-1:2017, *Household appliances network and grid connectivity – Part 1: General requirements, generic data modelling and neutral messages.*

BS IEC 62746-10-1:2018, *Systems interface between customer energy management system and the power management system – Part 10-1: Open automated demand response.*

ISO 15118 series, *Road vehicles — Vehicle to grid communication interface. Part 1 available at https://www.iso.org/standard/69113.html (last viewed 3 February 2020).*

IEC 61851 series, *Electric vehicle conductive charging system. Part 1 available at https://webstore.iec.ch/publication/33644 (last viewed 3 February 2020).*

IEC 61850, (all parts) *Communication networks and systems for power utility automation.*

IEC TR 62746-2:2015 *Systems interface between customer energy management system and the power management system – Part 2: Use cases and requirements*

IEC 62746-10-1:2018, *Systems interface between customer energy management system and the power management system – Part 10-1: Open automated demand response*

IEC 62746-10-3:2018 *Systems interface between customer energy management system and the power management system – Part 10-3: Open automated demand response – Adapting smart grid user interfaces to the IEC common information model*

IEC TR 61850-90-8:2016, *Communication networks and systems for power utility automation - Part 90-8: Object model for E-mobility. Available at https://webstore.iec.ch/publication/24475 (last viewed 3 February 2020).*

IEEE 802.11-2016, *IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Available at https://ieeexplore.ieee.org/document/7786995 (last viewed 3 February 2020).*

IEEE 2030.5-2013, *Smart Energy Profile 2.0 Application Protocol Standard. Published 11 November 2013. Available at https://standards.ieee.org/standard/2030_5-2013.html (last viewed 3 February 2013).*

PAS 1879 (in preparation)

prEN50491-12-2

Other publications

[1] EEBUS SHIP Available at https://www.eebus.org/en/media-downloads/#specifications (last viewed 3 February 2020).

[2] Zigbee Smart Energy Standard, Document 07-5356-19, copyright ZigBee Alliance, Inc. (2007-2014). Available at https://zigbeealliance.org/wp-content/uploads/2019/11/docs-07-5356-19-0zse-zigbee-smart-energy-profile-specification.pdf.

[3] Smart Metering Implementation Programme: GB Companion Specification (GBCS), latest edition, 4 July 2019. Available at https://smartenergycodecompany.co.uk/the-developing-sec/ (last viewed 3 February 2020).

[4] Open Charge Point Protocol (OCPP 2.0.1), Copyright © 2010 – 2019 Open Charge Alliance, Available at https://www.openchargealliance.org/downloads/ (last viewed 3 February 2020).

[5] The Ecodesign Preparatory Study on Smart Appliances (Lot 33) Task 7 Report. © European Union, October 2018. Available https://eco-smartappliances.eu/sites/ecosmartappliances/files/downloads/Task_7%282%29SEC2_22102018_FINAL.pdf (last viewed 3 February 2020).

[6] Latest versions of SMETS (and GBCS) and DCC User Interface Specification – https://smartenergycodecompany.co.uk/the-smart-energy-code-2/.

[7] Technical and Business Architecture Documents – https://smartenergycodecompany.co.uk/the-business-architecture-document-bad/.

[8] DCC User roles https://www.smartdcc.co.uk/customer-hub/about-dcc-users/.

[9] Security and privacy obligations overview https://smartenergycodecompany.co.uk/about-security-and-privacy-obligations.

[10] Communications Hubs Technical Specifications.

[11] Smart Metering Equipment Technical Specifications.

[12] SMETS2 version 5.

[13] Balancing and Settlement Code. Available at https://www.elexon.co.uk/bsc-and-codes/bsc-related-documents/codes-of-practice/.

[14] Secure Design Best Practice Guides, IoT Security Foundation. Release 2, November 2019.

[15] OpenADR 2.0 Profile Specification, OpenADR Alliance, copyright 2011-2012. Available at https://www.openadr.org/specification.

[16] OASIS Energy Interoperation 1.0, © OASIS Open 2014, published in 2014 available at http://docs.oasis-open.org/energyinterop/ei/v1.0/energyinterop-v1.0.html.

[17] European Commission, Study on ensuring interoperability for enabling Demand Side Flexibility. Published 2018, ISBN 978-92-79-91255-9.

[18] ETSI TS 103 264 V1.1.1 SmartM2M; "*Smart Appliances; Reference Ontology and oneM2M Mapping*".

[19] ETSI TS 103 410-1 V1.1.1 SmartM2M; "*Smart Appliances Extension to SAREF; Part 1: Energy Domain*".

[20] EEBus SHIP TS Specification v1.0.1, EEBus Intiative, 2018.

Further reading

CENELEC EN50631-1:2017, *Household appliances network and grid connectivity. General Requirements, Generic Data Modelling and Neutral Messages.*

IEC 62746-10-1, *Systems interface between customer energy management system and the power management system - Part 10-1: Open automated demand response. Published 19*

November 2018. Available at https://webstore.iec.ch/publication/26267 (last viewed 3 February 2020).

Code of Practice for Consumer Internet of Things (IoT) Security, *Department of Digital, Culture, Media and Sport, Crown copyright 2018, published October 2018. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf (last viewed 3 February 2020).*

