PAS 1878:2021

Energy smart appliances – System functionality and architecture – Specification

Department for Business, Energy & Industrial Strategy

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2021.

ISBN 978 0 539 05131 5

ICS 03.100.70; 27.015; 91.140.50

Publication history

First published May 2021

Contents

Annexes

List of figures

List of tables

Foreword

This PAS was sponsored by the Department for Business, Energy and Industrial Strategy (BEIS) and the Office for Zero Emission Vehicles (OZEV). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 31 May 2021.

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

- The Alan Turing Institute
- Association of British Certification Bodies (ABCB)
- Association for Decentralised Energy (ADE)
- The Association of Manufacturers of Domestic Appliances (AMDEA)
- BEIS/OZEV
- British Electrotechnical and Allied Manufacturers' Association (BEAMA)
- Carbon Co-op
- Centrica plc
- Consumer and Public Interest Network (CPIN)
- CSO Confidential Ltd
- Energy Systems Catapult
- Green Energy Options Ltd (geo)
- Kaluza Ltd
- Kiwi Power
- Mixergy Ltd
- Moixa Technology Ltd
- Society of Motor Manufacturers and Traders (SMMT)
- Tech UK
- United Kingdom Accreditation Service (UKAS)
- University of Newcastle
- University of Warwick

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

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

PAS 1879:2021, *Energy smart appliances – Demand side response operation – Code of Practice.*

Information about this document

This publication can be withdrawn, revised, partially superseded or superseded.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 has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute 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, subject to an explicit consumer consent, of energy smart appliances (ESAs) on an electricity network in order to:

- match the short-term availability of intermittent renewable energy generation sources such as wind and solar;
- decrease the peak load on the electrical transmission and distribution networks 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 and network voltage, and help prevent network and generation outages; and
- to allow the offset of short-term market imbalances 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.

At longer timescales and with sufficient notice, consumer behaviour change can be achieved through electricity suppliers altering the tariff that electricity consumers pay, which encourages the use of appliances at times outside of peak demand or at times when excess generation capacity is expected to be available. This is called the "routine" method and is delivered through electricity suppliers setting time of use (ToU) tariffs. 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 known as the "response" 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. Such benefits might also be direct, additional benefits may accrue to consumers willing to invest in and adopt appliances containing the ESA functionality and communication capabilities. Consumers with ESAs can reduce their electricity costs by operating domestic appliances using the Routine method, and can earn revenues by allowing domestic appliances to be controlled flexibly using the Response method. 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 and PAS 1879:2021, such as optimization of rooftop solar self -consumption with appliances or battery storage, that can provide additional benefits for consumers. The IEC 60364 series of standards provide guidance on the information exchange within prosuming electrical installations, e.g. IEC TS 60364-8-3:2020, Table 1.

This PAS provides a technical specification that allows domestic appliances to operate in such a DSR system and it is intended to be read in conjunction with PAS 1879:2021, which provides recommendations for the provision of DSR services by service providers.

0.2 Demand side response and energy smart appliances

Response mode DSR requires communication between domestic appliances and a controlling entity, which itself communicates with the appropriate regulated electricity market participant. 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 is described in PAS 1879.

To provide DSR services, a domestic appliance can 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 ESAs 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.

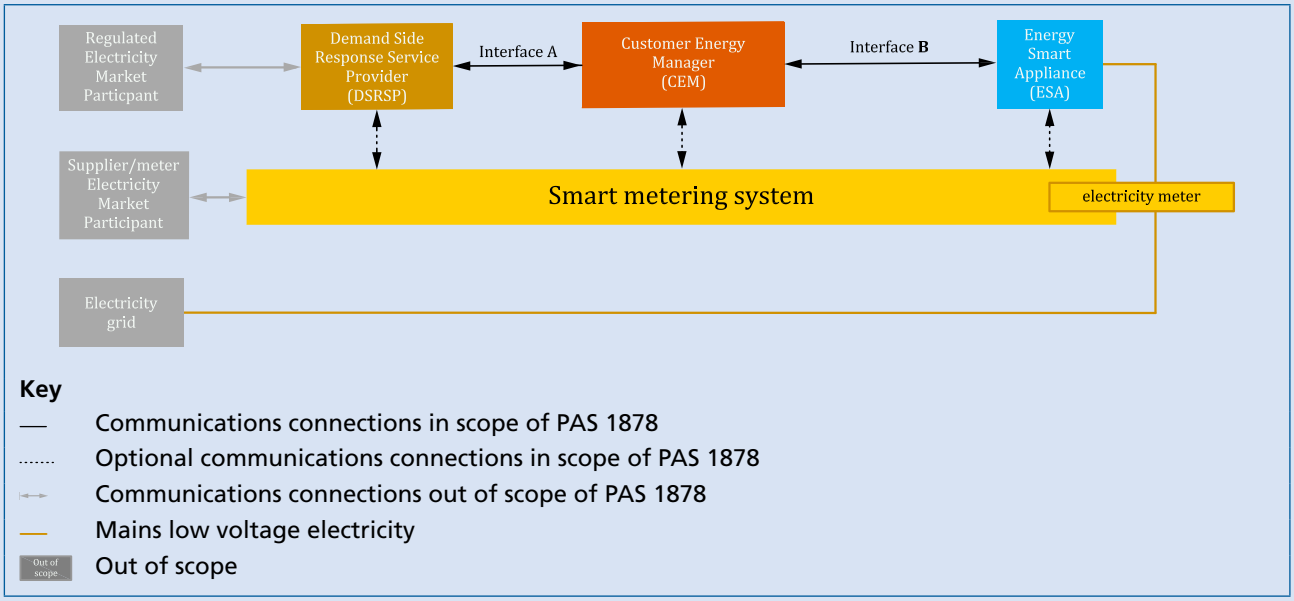
ESAs currently covered in this PAS include smart EV chargepoints, electric heating, ventilation and air conditioning (HVAC), domestic battery storage, wet appliances and cold appliances, but the ESA classification is not limited to these appliances; if an appliance that is not listed meets this specification 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.

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 are 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 turn up/down demand or supply to affect the power balance (e.g. energy arbitrage and reserve products) and products 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 often 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)", Energy Management Gateway and "ESA gateway (ESAG)" in Figure E.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 offers (taking into account consumer 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 offer 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 offers provided by the CEM on behalf of the ESAs that it manages.

d) Whenever the DSRSP is requested to perform a DSR operation, the DSRSP is able to select its chosen flexibility and time parameters from its portfolio of flexibility offers.

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 offers. The ESA implements this flexibility offer and enters response mode.

f) During the DSR event period:

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

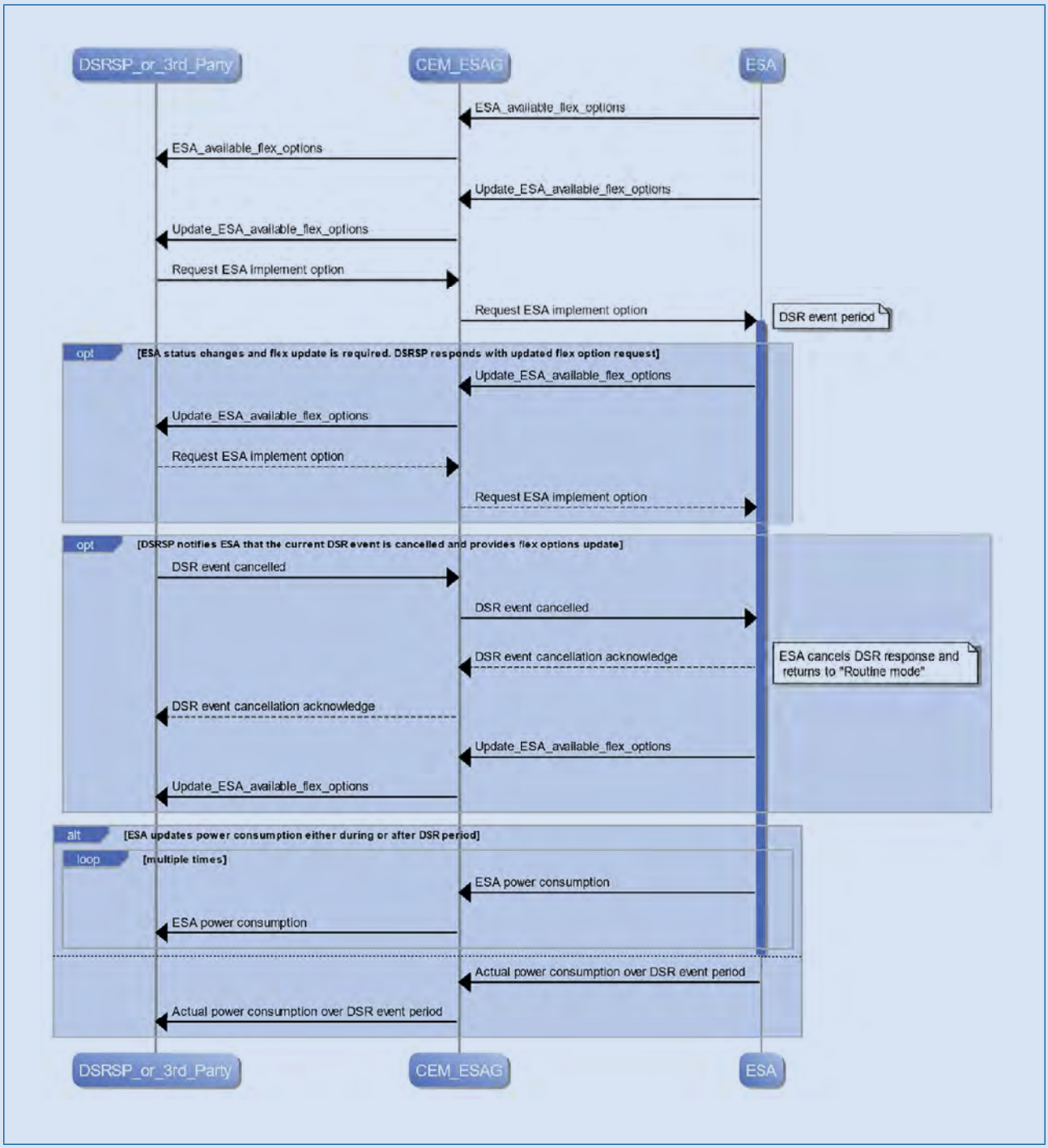
   3) depending upon the requirements of the DSRSP and subject to prior agreement, the ESA might periodically send power consumption information to the DSRSP;

   4) the consumer might change their preferences, which can in turn override the ESA flexibility offer and require the ESA to return to its routine mode.

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 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 (see **5.3.5.2.5**). 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 informative trust modelling exercise 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.

NOTE 1 *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.*

NOTE 2 *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. Attention is drawn to Schedule 7 of the Electricity Act 1989 [1] and the Measuring Instruments Regulations 2016 [2]. In the UK, the Balancing and settlement code [3] defines codes of practice which provide further details on settlement metering requirements for consumer electricity supply.*

NOTE 3 *A regulated electricity market participant requesting DSR services might require the DSRSP to evidence delivery of DSR services. This might require an ESA to provide information regarding its power consumption to the DSRSP.*

0.6 Alignment with standards

Standardization of domestic DSR is currently at an immature stage in some areas 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 P*erformance of household and similar electrical appliances*.

This page is deliberately left blank.

1 Scope

1.1 In 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 domestic or small business settings[1)]:

- cold appliances (see **3.1.6**);
- wet appliances (see **3.1.6**);
- heating, ventilation and air conditioning (HVAC) appliances (see **3.1.19**);
- smart EV chargepoints (see **3.1.28**); and
- battery storage.

1.2 Out of scope

This PAS does not cover:

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

1.3 Intended audience for this PAS

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.

NOTE *The specified characteristics of an ESA are complementary with the DSR environment in which it operates, which will be described in PAS 1879, as the characteristics enable the ESA to perform DSR-based activities.*

[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 [4].

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[2]. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Standards publications

BBS EN ISO/IEC 27000:2018 *Information technology – Security techniques – Information security management systems – Overview and vocabulary* FIPS 186-4, Digital Signature Standard

EN 303 645, v2.1.1 (2020-04), Cyber Security for Consumer Internet of Things: Baseline Requirements[3]

Non-standards publications

[N1] DCUSA LTD, *Distribution and Connection Use of System Agreement Document, v12.8 Pre-Release_Public.* London. 15 December 2020.[4]

[N2] National Cyber Security Centre (NCSC). *Implementing the Cloud Security Principles,* v1.0. 17 November 2018.[5]

[N3] National Institute of Standards and Technology (NIST). Special Publication 800-56A, Revision 2: *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.* Barker, E., Chen, L., Roginsky, A., Smid, M., May 2013.

[N4] Internet of Things Security Foundation (IoTSF). *Secure Design Best Practice Guides, Release 1.2.1.* Day, J., Shepherd, R., Kearney, P., Storer, R., December 2018.

[N5] National Institute of Standards and Technology (NIST), FIPS 140-2, Security Requirements for Cryptographic Modules[6]

[N6] Internet Engineering Task Force (IETF), RFC 8915, Network Time Security for the Network Time Protocol. 2020.[7]

[2] Documents that are referred to solely in an informative manner are listed in the Bibliography.
[3] Available at https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf
[4] Available at https://www.dcusa.co.uk/dcusa-document/
[5] Available at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles
[6] Available at https://csrc.nist.gov/publications/detail/fips/140/2/final.
[7] Available at https://tools.ietf.org/html/rfc8915

3 Terms, definitions and abbreviated terms

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:

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[i] [5] which was granted by the Department for 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, and acting in agreement with, regulated electricity market participants

3.1.12 demand side response service provider (DSRSP)

organization using ESAs to provide demand side-related energy management services to regulated electricity market participants

3.1.13 electric vehicle (EV) chargepoint

equipment enabling the recharging, or in the case of vehicle to grid (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 that 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 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 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

3.1.25 network physical interface

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

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 requirements in this PAS

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 any device in the home that is authorized to communicate with the smart meter

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)

functionality in GB smart metering that will connect to the HAN via the Communications Hub and is 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 Abbreviated terms

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

APC	auxiliary proportional controller
CA	certification authority
CAD	consumer access device
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
DUIS	DCC User Interface Specification
ESA	energy smart appliance
ESAG	energy smart appliance gateway
ESME	Electricity Smart Metering Equipment
EV	electric vehicle
HAN	home area network
HCALCS	HAN connected auxiliary load control switch
HEMS	home energy management system
HTTPS	secure hypertext transfer protocol
HVAC	heating ventilation and air conditioning
IoT	Internet of Things
mDNS	Multicast Domain Name System
NTS	Network Time Security
OCPP	Open Charge Point Protocol
OpenADR	Open Automated Demand Response
PII	Personal Identifiable Information
PKI	public key infrastructure
SAPC	standalone auxiliary proportional controller
SMHAN	smart meter home area network
TLS	transport layer security
ToU	time of use
TSO	transmission system operator
UART	universal asynchronous receiver-transmitter
USB	universal serial bus
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 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, PD IEC/TR 61850-90-8:2016 and BS EN 50491-12-1:2018), as described in **Annex E**.*

The ESA is a physical appliance, an edge processing device, making use of energy smart functionality and is sited on the consumer premises. The CEM is a logical entity providing energy management functionality and may be sited either on the consumer premises or externally to the consumer premises and either as standalone equipment or as part of other equipment including the ESA itself. The DSRSP is a business entity logically connected to a number of ESAs via their CEMs and is sited externally to the consumer premises.

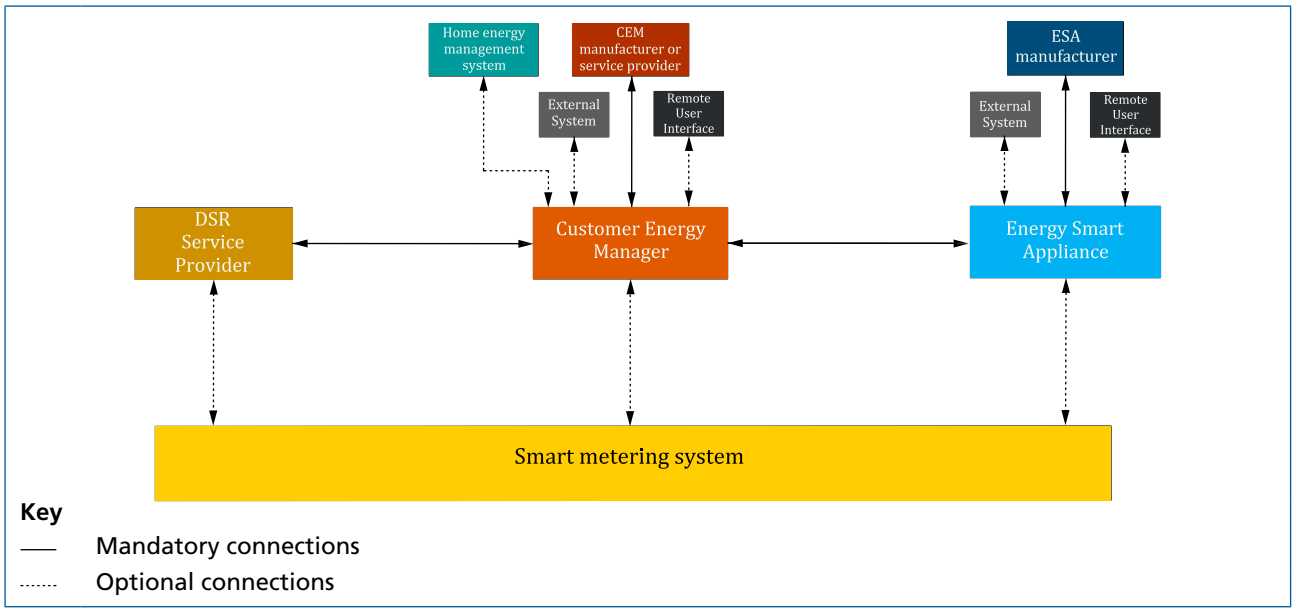
The ESA and CEM provide user interfaces for their energy smart functionality and status which allow the consumer (owner or user of an ESA) to interact with the ESA, CEM and the DSR services provided by the DSRSP.

A CEM is connected to only one DSRSP at any one time. An 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, denoted as the appliance controller in Figure 4. The appliance controller shall send and receive information, and receive requests, across Interface B and the Manufacturer Interface via its Physical Network 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 **5.1.2** (Interfaces A and B, the Manufacturer Interface and the User Interface) and might be used to support the network logical interfaces described in **5.1.3**. All network logical interfaces shall be logically separate from each other. The ESA shall connect to its manufacturer (or service provider) portal. This connection shall be used to securely download firmware and software updates.

NOTE 1 *This connection might also be used for other services.*

An ESA shall send registration, de-registration, authentication, flexibility offer, flexibility offer cancellation 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 apply them to Interface A without loss of information or corruption, in accordance with Clauses **5** and **6**.

An ESA shall receive registration, de-registration, authentication, flexibility offer request, flexibility offer cancellation and status messages from the DSRSP via its associated CEM.

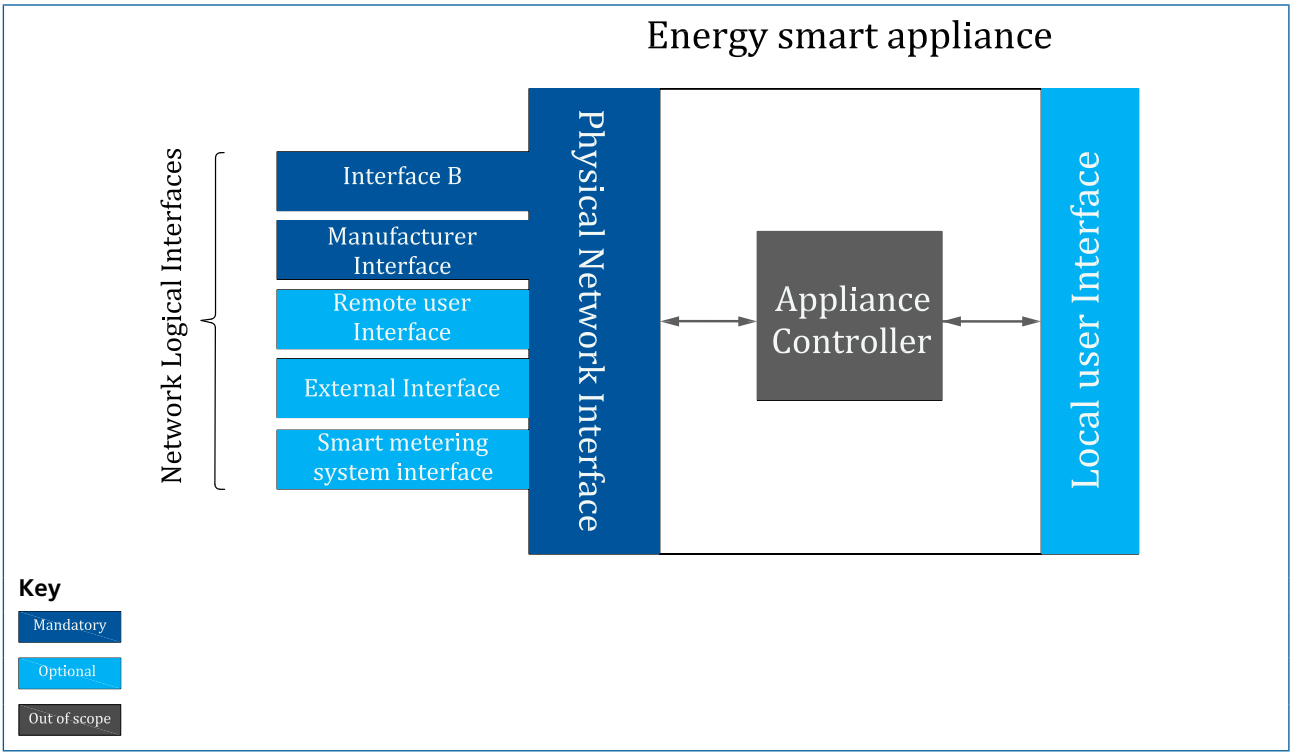
An ESA shall connect to no more than one CEM at any given time.

The ESA shall support a local (built-in) and/or remote 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 2 *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 3 *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 be instantiated either as part of an ESA or in another device in the home or in the cloud.

The CEM shall connect to its manufacturer (or service provider) portal. This connection shall be used to securely download firmware and software updates and might be used for other services.

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 **5.3**.

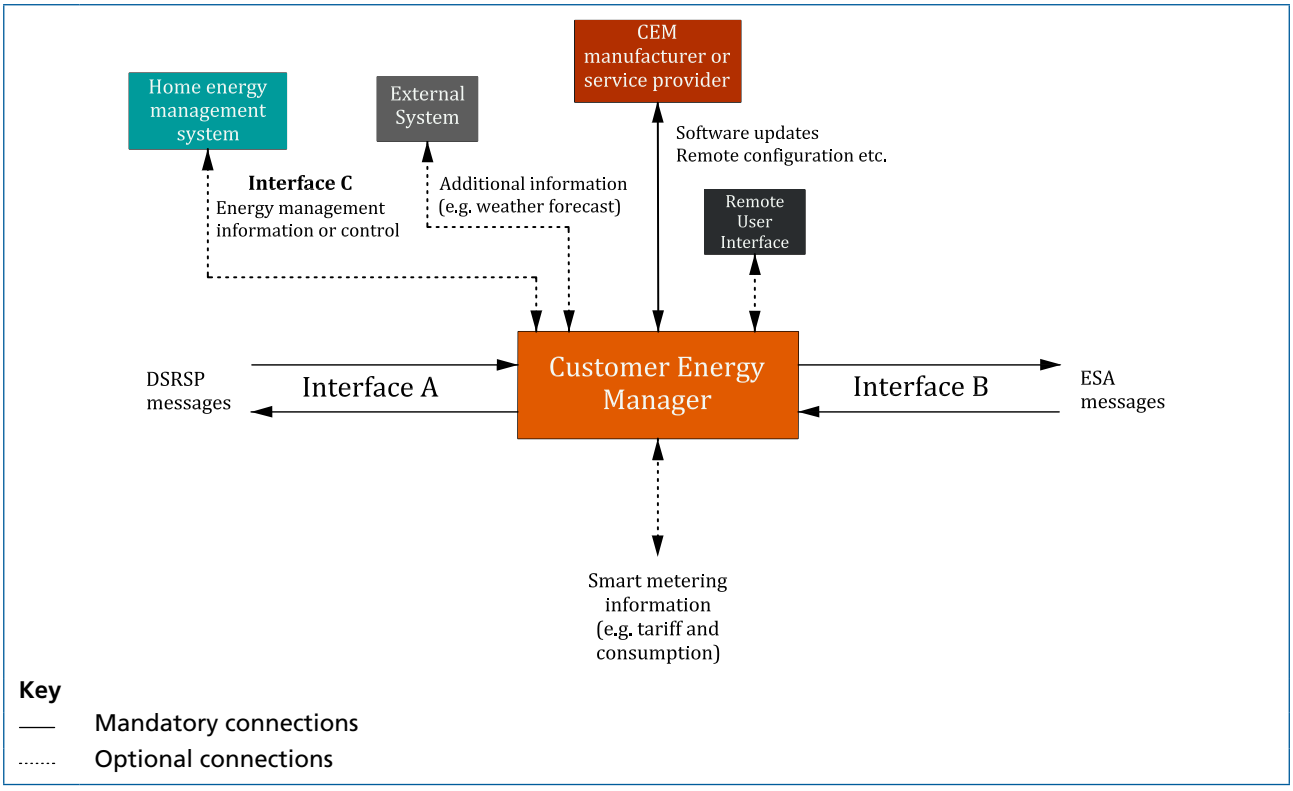
The CEM shall connect to no more than one DSRSP but shall be able to connect to at least one ESA at any given time.

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.

Figure 5 – CEM interfaces



The CEM may 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 **5.3.5.2**.

The CEM might form part of a Home Energy Management System (HEMS) in order to provide enhanced energy management services including those related to DSR and, if so, shall ensure that it is able to provide services as described in this PAS in addition to these enhanced energy management services.

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**).*

4.3 Demand side response service provider (DSRSP)

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

The DSRSP receives sets of flexibility offers from each of the active 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 ESA via the associated 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 Regulated Electricity Market Participants to provide DSR services. These participants 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 Regulated Electricity Market Participants and DSRSPs, and their relationship with ESAs, is described in more detail in PAS 1879.*

4.4 Manufacturer or service provider

Both the CEM and the ESA shall connect to their respective manufacturer or service provider portals. These portals shall provide secure software/firmware updates and device certificate management functionality as a minimum over a secure connection, as described in Clause **6**.

4.5 Remote user interface

The optional CEM or ESA remote user interface shall, as a minimum, provide access to information and controls required for the Consumer to engage in DSR services and allow the Consumer to provide their preferences for CEM or ESA operation and DSR service provision. The remote user interface shall give the consumer the ability to manually override, in real-time, current and planned DSR operations. The CEM or ESA and their respective remote user interfaces shall connect securely as described in Clause **6**.

4.6 Home energy management system (HEMS)

A HEMS and its associated CEMs shall connect securely as described in Clause **6**.

NOTE 1 *Figure B.5 shows an architecture for Interface C and HEMS integration.*

NOTE 2 *The optional home energy management system might provide energy management functionality additional to that provided by the CEM, provide additional information or requests for use by the CEM, or coordinate the operation of two or more CEMs associated with a premises.*

NOTE 3 *Connection of multiple CEMs with a single HEMS over a standardized interface might allow the energy management (including DSR) coordination of multiple ESAs within a single premises.*

5 Communications and messaging

*COMMENTARY ON CLAUSE **5***

*This Clause specifies minimum data model, message sequencing and underlying communications protocols, for Interface A in order to support interoperability between the DSRSP and CEM. Furthermore, this interoperable Interface A definition meets the cyber-security requirements described in Clause **6**.*

5.1 Interface architecture

5.1.1 General

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

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

5.1.2 Mandatory interfaces

5.1.2.1 Interface A

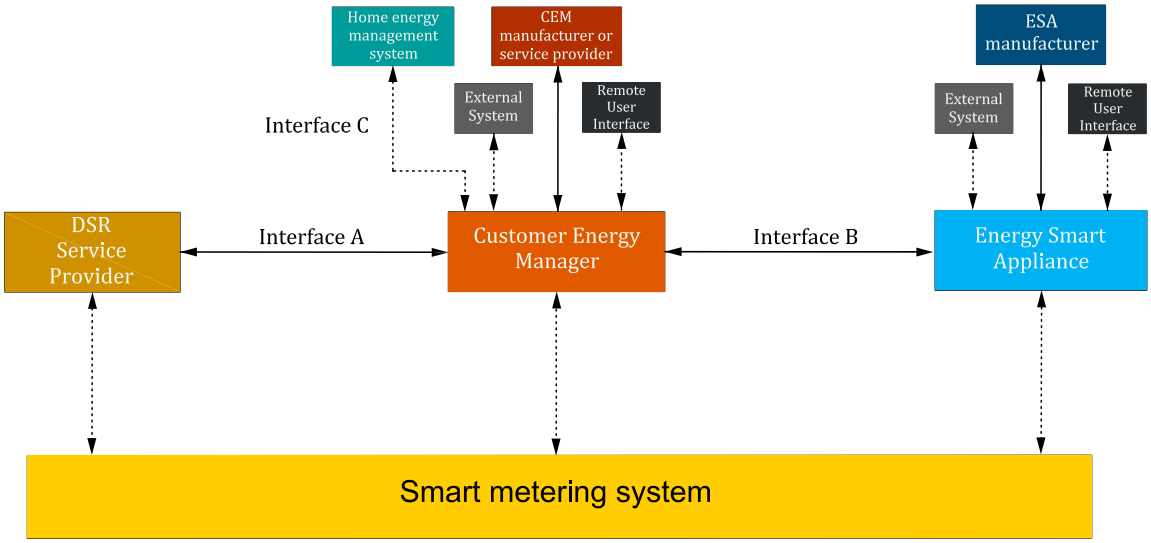
The DSRSP and the CEM shall exchange information relating to device registration, de-registration, flexibility offers, DSR events, status and cyber-security breaches across Interface A. Any DSRSP shall be able to communicate with any registered CEM, and vice versa, using Interface A.

***NOTE** 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. See **3.1.21** for a definition of interoperability.*

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

Interface A shall be implemented as specified in Annex **F**.

Figure 6 – Communications interfaces



5.1.2.2 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 with no loss or corruption of 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**.

5.1.2.3 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 **5.3.2** and to indicate that the CEM or ESA is to de-register.

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

5.1.2.4 User interface

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

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

5.1.3 Optional interfaces

5.1.3.1 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**.

5.1.3.2 Smart metering system interface

*COMMENTARY ON **5.1.3.2***

*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**.*

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

5.1.3.3 Interface C

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

***NOTE 1** A CEM can connect to a home energy management system (HEMS) over Interface C. As described in **4.2** and **4.6**, the interaction of a CEM and HEMS might provide additional energy management functionality.*

***NOTE 2** This interface might be standardized in the future.*

5.2 Communications architecture

*COMMENTARY ON **5.2***

The logical functional architecture described in this PAS consists of an ESA within the consumer 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 with no loss or corruption of information.

***NOTE 1** It is recommended that Interface B uses comparable data and message models to Interface A.*

***NOTE 2** 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 [6] 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. *Consumer 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 (four CEM operating modes)*
6. *Exception conditions*
7. *De-registration*

5.3.1 Consumer registration with DSRSP

*COMMENTARY ON **5.3.1***

In this phase, the Consumer 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 Consumer shall be able to begin the registration process for the DSR 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 Consumer with information that is to be used during the CEM and ESA to DSRSP service authentication and registration processes.

This information shall include:

a) DSRSP authorization code;

b) CEM service provision authorization code (if a remote CEM is used); and

c) 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 **6.14.2.2**. 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 **6.14.2.2.2** (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 Consumer (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 including 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

*COMMENTARY ON **5.3.3***

*The detailed process requirements for the registration of the CEM and ESA with the DSRSP are provided in **6.14.2.3** (DSRSP and CEM), but are summarized below.*

a) A CEM and ESA shall be registered to only one DSRSP at any given time. A CEM or ESA shall de-register with its existing DSRSP before registering with a new DSRSP.

b) A CEM or ESA shall communicate only with the registered DSRSP and shall not be capable of communicating with any other (e.g. previously registered) DSRSP.

c) Prior to registering with a DSRSP, the ESA shall delete any existing information relating to any previous DSRSP registration (DSRSP URL, DSRSP certificate etc.)

d) The CEM and DSRSP shall mutually authenticate using PKI over Interface A.

e) The CEM shall send its manufacturer name and serial number to the DSRSP over Interface A for validation.

f) The CEM shall send its manufacturer name, serial number, EUI-64, firmware version and firmware installation date to the DSRSP over Interface A.

g) The CEM shall send the ESA manufacturer name, 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 ESA, CEM and DSRSP are said to be registered and 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

5.3.5.1 General

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 a 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; and

g) indicate to the DSRSP that it has cancelled the previously selected flexibility offer.

The CEM shall pass information between the 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 .

5.3.5.2 CEM and ESA operating modes

5.3.5.2.1 General

During Normal Operation phase the CEM and ESA shall be capable of operating in any of the modes described in **5.3.5.2.2** to **5.3.5.2.5**.

5.3.5.2.2 Mode 1: Routine mode

The CEM shall be able to perform energy management functions and 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 1** The energy management functions supported by the CEM and ESA, and the non-DSR related Interface B functionality required are beyond the scope of this PAS.*

***NOTE 2** The CEM might connect with a Home Energy Management System (HEMS) over Interface C (see **4.6** and **5.1.3.3**) in which case the HEMS might be able to optimize energy usage across a coordinated set of CEMs and ESAs.*

5.3.5.2.3 Mode 2: Response mode

The ESA shall immediately enter Mode 2 (Response mode) once it has acknowledged to its registered DSRSP that it will be accepting and performing a valid flexibility offer, by sending a valid "flexibility offer request acknowledgement".

The ESA shall continue to send flexibility offer update messages to its registered DSRSP via its registered CEM.

The ESA shall prioritize its Mode 2 operation above its Mode 1 operation in that during the flexibility offer period the ESA shall not accept any requests from the CEM if the requests result in the ESA power consumption forecast contradicting that of the currently active flexibility offer.

The CEM shall immediately enter Mode 2 (Response mode) whenever it receives an authenticated and validated "flexibility offer request acknowledge" message from one of its ESAs to the registered DSRSP.

The CEM shall not include in its related HEMS functionality any of its registered ESAs that are currently in Mode 2.

The CEM shall continue to include in its related HEMS functionality any of its registered ESAs that are currently in Mode 1.

The ESA 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.

5.3.5.2.4 Mode 3: Consumer override

The ESA shall enter Mode 3 whenever it receives a manual override (i.e. modify, decline or cancel) from the Consumer.

In Mode 3, the ESA shall allow the Consumer to override any Mode 1 (routine) or Mode 2 (response) 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; or
b) rejection of a requested operation; or
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.

If the Consumer override involves a request rejection or event cancellation of a Mode 2 operation, the ESA shall send a "flexibility offer request rejected" or "cancel flexibility offer" (**5.4.5.1.6**) message to the DSRSP, via the CEM, and immediately revert to Mode 1 (Routine mode). The CEM shall authenticate and decrypt the "flexibility offer cancel" message received from the ESA over Interface B and, if authenticated and validated, shall both re-package the message, send to the DSRSP over Interface A and note that the ESA has transitioned to Mode 1. The CEM shall now include the ESA in any non-DSR HEMS operations as it sees fit.

If the Consumer override involves a request rejection or event cancellation of a Mode 1 operation, the ESA shall send a "Mode 1 request rejected" or "Mode 1 operation cancelled" message to the CEM, (the format of these messages is beyond the scope of this PAS) and immediately revert to Mode 1 (Routine mode). The CEM shall authenticate and decrypt the "flexibility offer cancel" message received from the ESA over Interface B and, if authenticated and validated, shall note that the ESA has transitioned to Mode 1. The CEM shall now include the ESA in any non-DSR HEMS operations as it sees fit.

5.3.5.2.5 Mode 4: Failsafe

The CEM and ESA control logic shall ensure that the CEM and ESA do not perform in a manner that can lead to an unsafe, harmful or otherwise hazardous situation. Whenever such a condition is imminent, the CEM and ESA shall transition into a failsafe state (Mode 4).

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.

The details of the behaviour of the ESA in Mode 4 shall be determined by the manufacturer but shall always ensure that the ESA enters a safe state. The ESA shall always attempt to inform the CEM that it is entering Mode 4 (under some conditions, there might not be time to do so) by sending an encrypted and signed "entering failsafe" message and an encrypted and signed "Cancel flexibility offer" message. The ESA shall indicate that it has entered Mode 4 on its User Interface.

Upon receiving an authenticated and valid "Cancel flexibility offer" message over Interface B from a registered ESA, a CEM shall re-package the message, send to the DSRSP over Interface A and note that the ESA has transitioned to Mode 4.

Upon receiving an authenticated and valid "entering failsafe" message over Interface B from a registered ESA, a CEM shall note that the ESA has transitioned to Mode 4 and exclude the ESA from any DSR or non-DSR HEMS operations.

The ESA shall exit Mode 4 only when safe to do so by sending a valid (encrypted and signed) flexibility offer update message (the ESA shall transition to Mode 2) or appropriate Interface B specific notification (beyond the scope of this PAS, the ESA shall transition to Mode 1).

The details of the behaviour of the CEM in Mode 4 shall be determined by the manufacturer or service provider but shall always ensure that the CEM enters a safe state. The CEM might attempt to inform the DSRSP that it is entering Mode 4 (under some conditions, there might not be time to do so) by sending an encrypted and signed "entering failsafe" message. The CEM shall indicate that it has entered Mode 4 on its User Interface.

5.3.5.3 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 1.

5.3.6 Exception conditions

The ESA shall:

a) detect any attempt by unauthorized parties to compromise its operation or to access sensitive information according to **6.13.1** and;

b) determine if a failsafe condition has occurred and, if so, transition to Mode 4 (as described in **5.3.5.2.5**).

c) Attempt to resolve any issue arising from a) and b) above, issuing a flexibility offer update message if appropriate. If a safe resolution is not possible, then the ESA shall transition to (or remain in) Mode 4 (as described in **5.3.5.2.5**). The ESA shall exit Mode 4, only when safe to do so and when instructed by the Consumer, according to **5.3.5.2.5**.

The CEM shall:

a) detect any attempt by unauthorized parties to compromise its operation or to access sensitive information according to **6.13.1**;

b) determine if a failsafe condition has occurred and, if so, transition to Mode 4 (Failsafe mode); and

c) attempt to resolve any issue arising from a) and b) above. If a safe resolution is not possible, then the CEM shall transition to (or remain in) Mode 4 (as described in **5.3.5.2.5**). The CEM shall exit Mode 4, only when safe to do so and when instructed by the Consumer, according to **5.3.5.2.5**.

Table 1 – Operating modes

Priority	Operating mode
1	ESA failsafe
2	Consumer override [A)]
3	Response mode
4	Routine mode

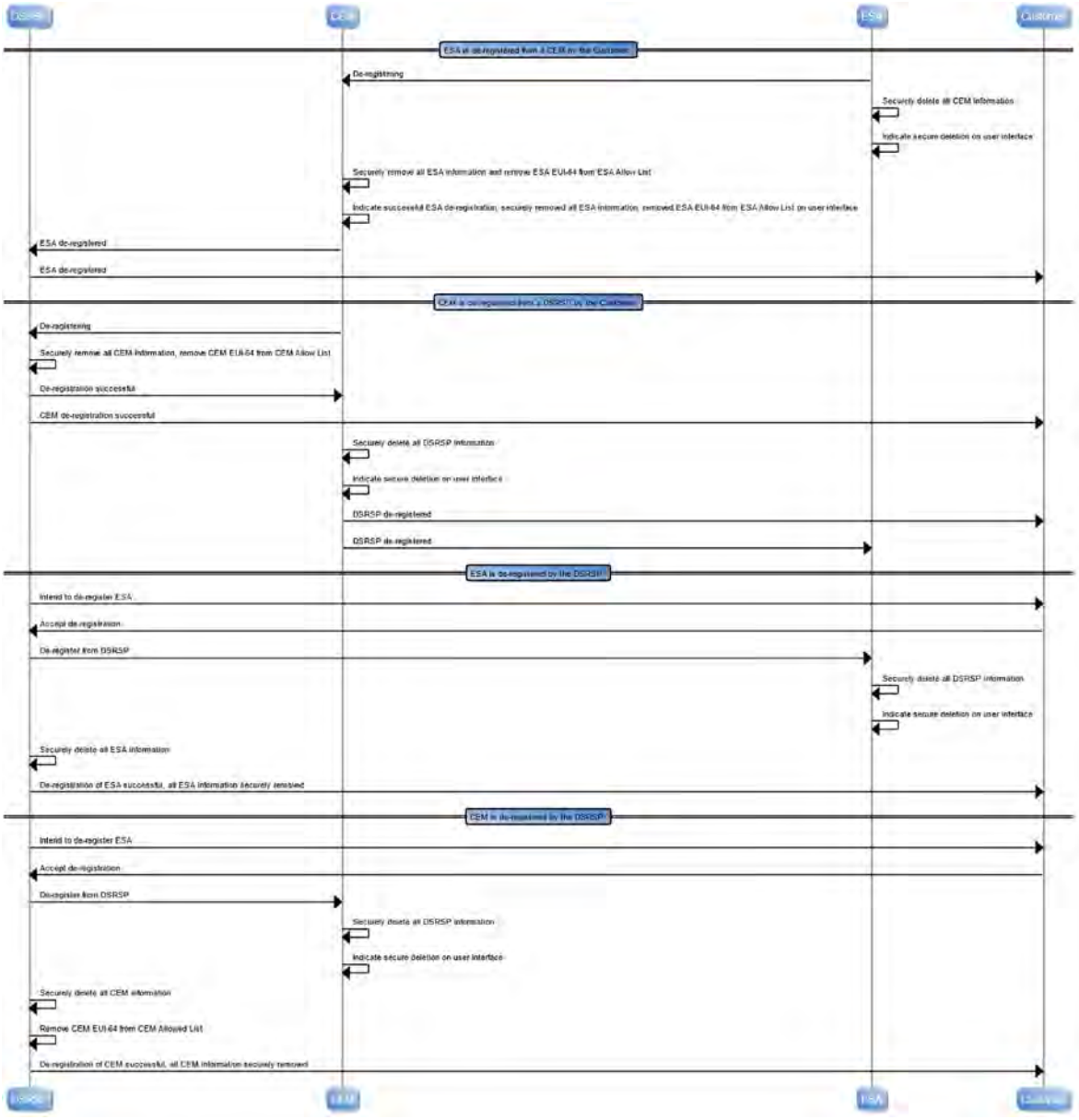
[A)] The consumer sets their preferences, which will be automatically considered in Routine and Response Modes. This case specifies a subsequent manual intervention to override planned operation.

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 consumer

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 Consumer 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 the Consumer that its information removal process is complete.

The CEM shall securely remove all information related to the ESA, logging all actions, before sending an "ESA de-registration notification" message to the DSRSP over Interface A.

The CEM shall receive an encrypted and signed "ESA de-registration acknowledged" message over Interface A to indicate that the DSRSP has securely removed all information related to the ESA and logged all actions.

If the CEM does not receive an "ESA de-registration acknowledged" message within five minutes of sending the "ESA de-registration notification" message then the CEM shall re-send the "ESA de-registration notification" message. If necessary, this process shall be repeated two more times. If no "ESA de-registration acknowledged" message is received within five minutes of the final re-try, then the CEM shall assume that de-registration has been successful and proceed accordingly.

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

When a CEM is being de-registered from a DSRSP by the Consumer, the CEM shall send a "de-registering" message to the DSRSP over Interface A. On receipt of an encrypted and signed "de-registration successful" message over Interface A, 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 Consumer and to the ESA that it has been de-registered from the DSRSP.

NOTE 1 *When a CEM or an ESA is being de-registered by the DSRSP, the DSRSP should inform the consumer that it has received the de-registration request 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 2 *The DSRSP should securely remove all ESA information and inform the Consumer 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 Consumer 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 Consumer 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:

a) Consumer registration with DSRSP (excluded from information model);

b) CEM and ESA mutual authentication;

c) Registration of the CEM and the ESA with the DSRSP;

d) Initialization;

e) Normal operation (four CEM operating modes);

f) Exception conditions;

g) De-registration.

5.4.1 General

A DSRSP and CEM shall act upon and generate all the information listed below in **5.4.2** and **5.4.3** in order to be compliant with Interface A. The information listed below shall form the basis of a data model.

An ESA shall act upon all information listed below in **5.4.3** generated by the DSRSP and shall generate the information listed below that corresponds to the capabilities of the ESA.

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 or corruption of information.

5.4.2 CEM and ESA mutual authentication

5.4.2.1 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
Interface B version	M	
ESA manufacturer name	M	
ESA unique serial number	M	
ESA EUI-64	M	
ESA firmware version	M	
ESA firmware installation date	M	

5.4.2.2 Interface A version

This information shall indicate the version of the Interface A specification supported by the CEM.

5.4.2.3 ESA manufacturer name

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

5.4.2.4 ESA unique serial number

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

5.4.2.5 ESA EUI-64

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

5.4.2.6 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).

5.4.3 Registration of the CEM and the ESA with the DSRSP

5.4.3.1 Information passed from the CEM to the DSRSP

The information in Table 3 shall be passed from the CEM to the DSRSP, in addition to that used for the PKI authentication process (as described in **6.14.2.3**), in order to allow the CEM and ESA to be registered with the DSRSP.

Table 3 – Information passed from the CEM to the DSRSP during the CEM/ESA registration process

Information element	Mandatory/ Optional	Note
Interface A version	M	
CEM manufacturer name	M	
CEM unique serial number	M	
CEM EUI-64	M	
CEM firmware version	M	
ESA manufacturer name	M	
ESA unique serial number	M	
ESA EUI-64	M	
ESA firmware version	M	

5.4.3.2 Interface A version

This information shall indicate the version of the Interface A specification supported by the CEM.

5.4.3.3 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.*

5.4.3.4 CEM unique serial number

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

5.4.3.5 CEM EUI-64

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

5.4.3.6 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).

5.4.4 Initialization

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

5.4.4.1.1 General

The information in Table 4 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 and shall be subject to the cyber security conditions described in **6.14.1**.

Table 4 – Information passed from the ESA to the DSRSP via the CEM during initialization

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

5.4.4.1.2 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. This shall be an enumerated value as defined in Table 5.

***NOTE** Subsequent versions of this PAS might include additional enumerations.*

Table 5 – Flexibility offer type enumeration values

Flexibility offer type	Enumeration value	Note
Forecast power profile	1	

5.4.4.1.3 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 one or both of the following types:

- instantaneous power consumption or production, sent to the DSRSP as a minimum periodicity value in seconds; 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, denoted by a periodicity value of 0.

5.4.4.1.4 ESA type

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

a) cold appliance;
b) wet appliance;
c) electric HVAC;
d) smart EV chargepoint; or
e) battery storage.

This information element shall use the enumerated values described in Table C.1.

5.4.4.1.5 ESA classification

The ESA classification information element shall indicate the maximum and minimum consumption and/ or production power of the ESA according to Tables C.3 and C.4; this information within the element is optional.

5.4.4.2 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 6 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 6 – 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

5.4.4.3 Preferred power reporting type

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

This information element shall consist of either:

a) instantaneous power consumption or production, provided as a periodicity value in seconds (not to exceed the minimum limit provided by the ESA); or

b) power consumption or production profile, denoted by a periodicity value of 0.

5.4.5 Normal operation

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

5.4.5.1.1 General

The information in Table 7 shall be passed from the ESA to the DSRSP, via the CEM, as necessary during Normal operation phase.

Table 7 – 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
Flexibility offer request acknowledgement	M	Contains the flexibility offer identifier
Cancel flexibility offer Entering failsafe	M M	Interface B only (see **5.3.5.2.5**)
Free text	O	DSRSP specific

5.4.5.1.2 Flexibility offers

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

a) forecast power profiles – at least the minimum required set of "least delayed" (LD), "intended operation" (IO) and "most delayed" (MD) forecast power profiles; and

b) frequency response capability indicator – indicating the ESA is able to move into a frequency response mode for a specified period. The state of this element shall indicate the frequency response capability of the ESA and is associated with a forecast power profile. Separate Frequency Response Capability indicators shall be provided for each of the LD and MD forecast power profiles.

The Frequency Response Capability indicator shall be defined as in Table 8.

Table 8 – Frequency response indicator values

Frequency Response Capability indicator value	ESA Frequency response capability
0	No frequency response capability
1	static frequency response capability
2	dynamic frequency response capability with a response linearly proportional to the frequency deviation
3	dynamic frequency response capability with a response proportional to the square of the frequency deviation
N	dynamic frequency response capability with a response proportional to (N-1)th power of the frequency deviation

The ESA shall inform the DSRSP, via the CEM, whenever the ESA power profile or associated frequency response status changes by sending a flexibility offer update. 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.*

5.4.5.1.3 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 **5.6** shall be met for actual instantaneous power value reporting.

5.4.5.1.4 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 **5.4.4.2**).

The requirements in **5.6** shall be met for actual instantaneous power value reporting.

5.4.5.1.5 Flexibility offer request acknowledgement

The ESA shall indicate its implementation of the selected flexibility offer chosen by the DSRSP by sending a flexibility offer request acknowledgement to the DSRSP.

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

5.4.5.1.6 Cancel flexibility offer

The "Cancel flexibility offer" information element shall be used by the ESA to indicate to the DSRSP that it is no longer implementing the previously selected flexibility offer. This message shall contain the flexibility offer identifier.

5.4.5.1.7 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.*

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

5.4.5.2.1 General

The CEM and ESA shall be able to receive and process the following information (shown 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	Includes optional execution duration value, communications timeout values.
DSR event cancelled	M	Includes cancelled flexibility offer identifier
Tariff	O	Country/ supplier-specific format

5.4.5.2.2 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.

If the ESA reports that it is capable of performing frequency response in the corresponding flexibility offer then the flexibility offer request shall include maximum frequency 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.*

This information element might include an execution period (the duration of which shall be less than or equal to the remaining duration available for the flexibility offer) or 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).

5.4.5.2.3 Cancel flexibility offer

The "Cancel flexibility offer" information element is used by the DSRSP to signal to the appropriate ESA that the ESA should cancel the current Flexibility offer (DSR event): this information element shall include the ESA flexibility offer identifier.

5.4.6 Exception conditions

5.4.6.1 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 or when requested by the DSRSP as described in **6.14.2.3**.

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

Information element	Mandatory/ Optional	Note
Security events log	M	

5.4.6.2 ESA to CEM security event log

This secure log contains events relating to possible ESA or CEM compromise. It is described in **6.11**.

5.4.6.3 Information passed from the CEM to the DSRSP and ESA

The following information, shown in Table 11, shall be passed from the CEM to the DSRSP whenever exception conditions arise or when requested by the DSRSP as described in **6.14.2.3**.

Table 11 – Information passed from the CEM to the DSRSP exception conditions

Information element	Mandatory/ Optional	Note
Security events log	M	Includes exception code

5.4.6.4 CEM to DSRSP security event log

This secure log contains events relating to possible ESA or CEM compromise. It is described in **6.11**.

5.4.7 De-registration

5.4.7.1 Information passed from the ESA to the CEM and DSRSP

The information in Table 12 shall be passed from the ESA to the CEM over Interface B whenever the ESA wishes to de-register from the CEM and DSRSP.

Table 12 – Information passed from the ESA to the CEM to indicate de-registration

Information element	Mandatory/ Optional	Note
De-registration request	M	Interface B only

5.4.7.2 De-registration request

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 **5.3.7.1**.

5.4.7.3 Information passed from the CEM to the ESA and DSRSP

5.4.7.3.1 General

A selection of the information in Table 13 shall be passed from the CEM to the ESA and DSRSP whenever the CEM or ESA wish to de-register.

Table 13 – Information passed from the CEM to the ESA and the DSRSP to indicate de-registration

Information element	Mandatory/ Optional	Note
CEM de-registration	M	CEM to DSRSP only
ESA de-registration notification	M	
De-registration confirmation	M	CEM to ESA only
De-registering	M	

5.4.7.3.2 CEM de-registration

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

5.4.7.3.3 ESA de-registration notification

The CEM shall send an "ESA de-registration notification" message to the DSRSP once it has received, authenticated and validated a "de-registration request" from one of its ESAs. This shall contain the identifier of the ESA and the CEM, according to **5.4.7.4.2**.

5.4.7.3.4 De-registration confirmation

The CEM shall send a "de-registration confirmation" message to the ESA in order to indicate that the ESA shall remove all information relating to the CEM and DSRSP, according to **5.3.7.1**.

5.4.7.3.5 De-registering

The CEM shall send a "de-registering" message to the DSRSP over Interface A to indicate that it is requesting de-registration, as described in **5.3.7.1**. The message shall contain the CEM identifier.

5.4.7.4 Information passed from the DSRSP to the CEM

5.4.7.4.1 General

The information in Table 14 shall be passed from the CEM to the ESA and DSRSP whenever the CEM or ESA wish to de-register.

Table 14 – Information passed from the DSRSP to the CEM during de-registration

Information element	Mandatory/ Optional	Note
ESA de-registration acknowledged	M	CEM to DSRSP only
De-registration successful	M	

5.4.7.4.2 ESA de-registration notification

The CEM shall receive an "ESA de-registration acknowledged" message over Interface A, in response to a previous "ESA de-registration notification" message, whenever the DSRSP is acknowledging the de-registration of an ESA, according to **5.3.7.1**. The message shall contain the ESA and CEM identifiers.

5.4.7.4.3 De-registration successful

The CEM shall receive a "de-registration successful" message over Interface A, in response to a previous "de-registration" message, whenever the DSRSP is acknowledging the de-registration of a CEM, according to Clause **5.3.7.1**. The message shall contain the CEM identifier.

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**) with optional frequency response service capability indicators.

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 shall provide a flexibility offer update to the DSRSP, via the CEM, whenever the ESA flexibility offer status changes for any of the minimum required set of power profiles and for any additional power profiles sent to the DSRSP from the ESA/CEM.

The flexibility offer and flexibility offer update shall include an identifier for each of the included profiles in addition to the ESA identifier.

The flexibility offer and flexibility offer update shall contain the same information.

A flexibility offer update shall contain whichever profile types (IO, MD, LD) are being updated.

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

- *consumer intervention, or optional external data update, or other change in parameters to ESA forecast calculation, resulting in a change of flexibility offer status;*
- *start of any active period in any profile (IO, MD, LD);*
- *end of any active period in any profile (IO, MD, LD).*

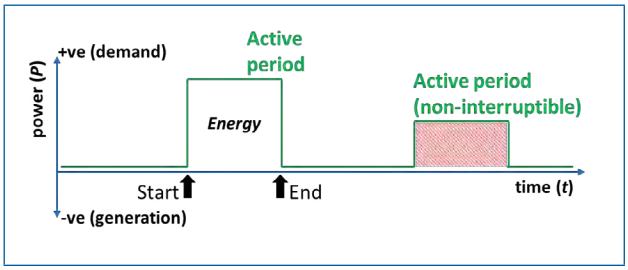
NOTE 2 *In order to minimize the number of updates required, this event-triggered update approach is specified as opposed to an approach of providing updates continuously at regular intervals.*

The ESA shall be able to receive messages from the DSRSP, via the CEM, 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 8.

Figure 8 – General form of a power profile



The ESA shall send an updated set of forecast power profiles as part of the flexibility offer update message whenever the status changes and these shall be forwarded to the DSRSP by the CEM.

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.*

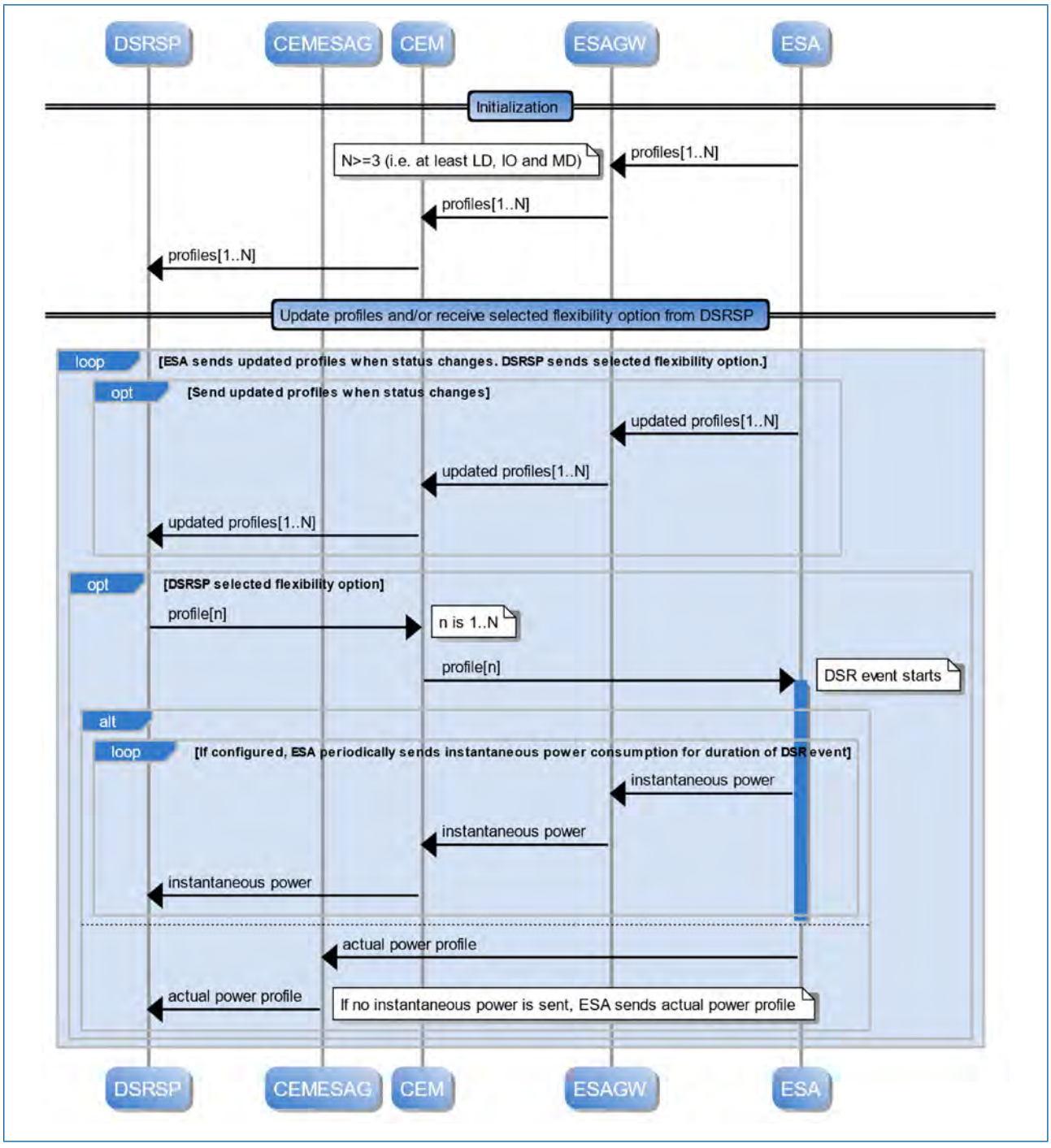
NOTE 2 *When the DSRSP wishes to initiate a DSR event period, it should determine the flexibility options available to it by examining the forecast power profiles, and select one. The DSRSP should then send a message including the index of the chosen forecast to the appropriate CEM.*

The CEM shall log all requests it receives over Interface A.

The ESA shall provide power consumption information to the DSRSP, via the CEM, 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 9.*

Figure 9 – Overall power forecast generation and selection process



5.5.4 Minimum set of forecast power profiles

5.5.4.1 General

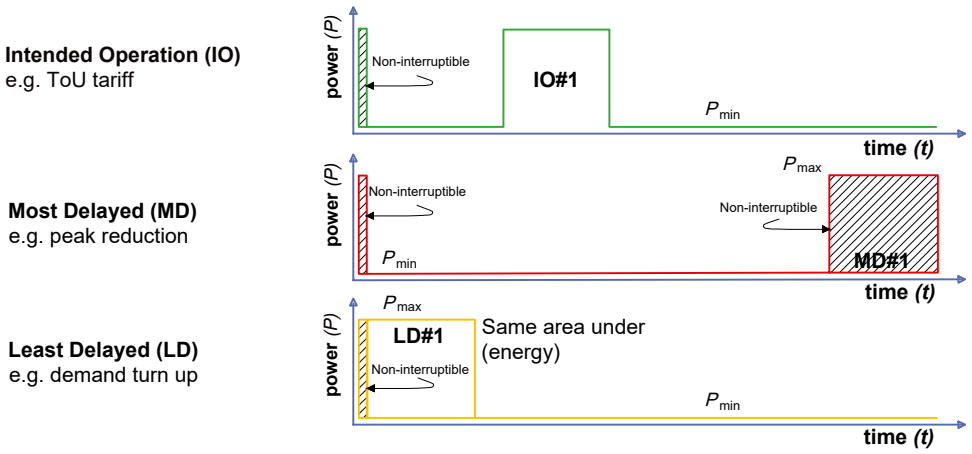
An ESA shall generate at least three forecast power profiles:

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

NOTE *An example of these three profile types is shown in Figure 10.*

All ESAs shall indicate forecast power consumption limits within the LD and MD forecast profiles.

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 (MD_P);
- least delayed production (LD_P).

ESAs able to produce power shall indicate forecast power production limits within the LD_P and MD_P forecast profiles.

An ESA may optionally have the capability to produce additional forecast power profiles such that the total number of forecast power profiles (including the mandatory forecast power profiles) shall not exceed 1000.

Forecast power profiles shall denote power consumption using positive power values and power production using negative power values.

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. including operation as part of a wider HEMS, under the control of the CEM (out of scope of PAS 1878) as described in **5.3.5**. 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 Calculating Intended Operation in Routine Mode

To avoid large simultaneous unwanted switches in load on the electricity network, the ESA shall be capable of applying a randomized offset to the profile start time when creating Intended Operation profiles.

The offset shall be applied only when the data source(s) used to calculate the Intended Operation profile does not already include a randomized offset.

The ESA shall be capable of applying a randomized offset in the range 0 seconds to 1800 seconds.

When operating in Great Britain, the ESA shall apply a randomized offset in the range 0 s to 600 s by default (unless specified otherwise in DCUSA, Schedule 8 [N1]). This randomized offset shall be applied only when the data source(s) used to calculate the Intended Operation profile does not already include a randomized offset.

The consumer override function specified in **5.3.5.2.4** 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:

a) the ESA shall calculate the initial IO, MD and LD forecast power profiles for a given flexibility forecast period as part of a flexibility offer;

b) these shall be sent to the DSRSP via the CEM as a flexibility offer update whenever their status changes or they expire;

c) 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

d) upon requesting a flexibility offer, the DSRSP can select either LD or MD as it sees fit and send the request to the ESA via the CEM, which shall respond as quickly as possible, either implementing the DSRSP's request or rejecting it if it is not applicable (i.e. a request that would result in unsafe, detrimental or otherwise abnormal behaviour).

5.5.5 Frequency response capability within 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 within the flexibility offer to the DSRSP via the CEM.

The ESA shall include a frequency response capability indicator in the flexibility offer, as defined in **5.4.5.1.2**.

If capable, the ESA shall be able to receive requests from the DSRSP including the frequency response information, as defined in **5.4.5.2.2**.

5.6 Actual power value or profile provision

An ESA shall be capable of measuring or calculating its power consumption/production value in W or kW (e.g. by using an internal measuring approach 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. Attention is drawn to Schedule 7 of the Electricity Act 1989 [1] covering use of Electricity Meters and The Measuring Instruments Regulations SI 2016/1153 [2]. In the UK the Balancing and Settlement Code [3] defines Codes of Practice which provide further details on metering requirements.*

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 1 kW each, with a measurement accuracy of 10%, will allow the total response of 10 MW 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 (**5.4.4.1.3**).

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 (**5.4.4.1.3**).

The ESA shall measure or calculate and report the power consumption/production values to meet the particular requirements of the DSRSP.

NOTE 3 *These requirements are based on the DSR service provided. Illustrative examples of DSR 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.

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 BS EN ISO/IEC 27000.*

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.

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

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

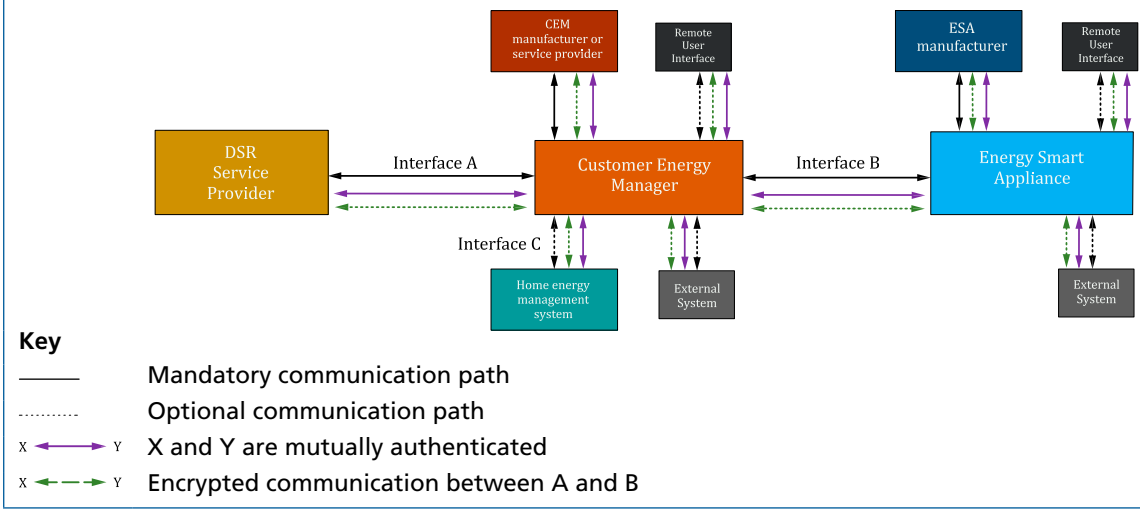
6.2 Cyber security architecture

*COMMENTARY ON **6.2***

*The relationship between the DSR architecture components and interfaces 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



As described in **5.1.2** the mandatory interfaces are:

- Interface A, between the DSRSP and CEM;
- Interface B, between the CEM and ESA;
- the manufacturer interface between the CEM and ESA and their respective manufacturer or service provider portals; and
- the remote user interface for the ESA.

The mandatory interfaces shall provide mutual authentication and encryption using TLS v1.3 (or later) and X.509 certificates. Information on cipher suites is provided in **F.8.2**.

As described in **5.1.3** the optional interfaces are:

- Interface C, between a HEMS and one or more CEMs;
- the external interface between the CEM and ESA and an external service provider; and
- the smart metering system interface.

Interface C and the external interface shall provide mutual authentication and encryption using TLS v1.3 (or later) and X.509 certificates. Information on cipher suites is provided in **Annex G**.

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

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.
- Connection to any other external sites shall be authenticated and shall use encrypted connections in accordance with internet security best practice and TLS v1.3 or later. The CEM and ESA execution environment shall class information received from such sites as insecure and apply the appropriate access, storage and execution right controls.

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.

6.3 General cyber security

The ESA and CEM shall conform to EN 303 645.

Any secrets relied upon for security (e.g., cryptographic keys, passwords), shall be unique to the ESA and CEM.

Any sensitive processes on the ESA and CEM (such as cryptographic functions) shall be made to be as confidential as possible, using trusted platform techniques [e.g., Trusted Execution Environment (TEE), Measured Boot].

Remotely hosted services [e.g., DSRSP, or CEM (when the CEM is in the cloud)], shall be designed to protect against Denial of Service (DoS) attacks.

Any cloud-based service used to host the DSRSP or CEM (when the CEM is in the cloud), shall be demonstrably secure in accordance with known good practice (e.g., NCSC's *Cloud Security Principles* [N2]).

The attack surface of the DSRSP, CEM and ESA shall be reduced by only presenting the interfaces and services required for normal operation of the device. Management and administrative functions shall be disabled and shall not be accessible to the normal user. It shall not be possible to make unauthorized connections to listening interfaces and services on the DSRSP, CEM or ESA.

6.4 Key generation

*COMMENTARY ON **6.4***

The following requirements are applied to the key pair generation process required by PKI.

Any long-term cryptographic key pairs shall be generated within the CEM and ESA only.

Private keys shall be stored within a secure area and no mechanism shall be provided for their export.

A cryptographically secure pseudo-random number generator shall be used in the key generation process.

A hardware random number generator should be used.

The pseudo-random number generator shall not be initialized using a timestamp and/or fixed data (such as serial number, EUI-64 etc.).

6.5 Product design, manufacture and supply chain

CEM and ESA manufacturers and vendors shall ensure that their design and business processes conform to best practice standards including BS EN ISO/IEC 27000.

The software development practices used by CEM and ESA manufacturers shall be governed by a secure software development lifecycle.

Software design shall be subject to best practice quality standards such as those produced by MISRA[8].

***NOTE** Other standards can be used if they can be shown to lead to the same results.*

6.6 Privacy

Any Personal Identifiable Information (PII) stored on the DSRSP, CEM and ESA shall be protected and handled in accordance with country-specific data protection legislation.

***NOTE** In the United Kingdom, attention is drawn to the General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018 [7].*

PII shall be stored in the Secure Storage Area of the CEM and ESA.

The end user of the ESA shall be able to remove any PII and any sensitive or unique cryptographic material i.e., through a factory reset function.

The Consumer shall provide permission to allow access to any specific information as part of the DSRSP contract.

6.7 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.

6.8 Protocols and configurations

TLS v1.3 or later with X.509 certificates shall be used over Interface A.

The set of TLS criteria specified in Table 15 shall be used over Interface A.

[8] Motor Industry Software Reliability Association

Table 15 – TLS criteria

Criteria	Version
Protocol	*TLS v1.3 (or later)*
Protocol Ciphers	*TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
Client Certificate Hash Algorithm	*SHA256*
Server Certificate Key	*RSA 2048 bit*
Server Certificate Hash Algorithm	*SHA256*

Resulting DerivedKeyingMaterial (as defined in NIST Special Publication 800-56A [N3]) shall only ever be used in relation to one Message Instance. Any Shared Secret that is not 'zeroized' shall be stored and used with the same security protections as Private Keys, i.e. in the Secure Storage Area.

***NOTE** A DSRSP may also additionally make use of IPSec for communications to a sub-contracted third party, as described in PAS 1879, **10.5.2.2**.*

6.9 Secure boot

The ESA and CEM shall ensure software/firmware integrity by operating secure boot processes, such as recommended in EN 303 645 and the IoT Security Foundation's *Secure Design Best Practice Guides* [N4].

6.10 Software and firmware updates

*COMMENTARY ON **6.10***

For the purposes of this subclause, "manufacturer/service provider" includes reference to any authorized third parties acting on behalf of the manufacturer/service provider.

***NOTE** The firmware updates shall be hashed and signed before being sent to the CEM or ESA for authentication in addition to the firmware image itself.*

The ESA and CEM shall be provided with the latest software and firmware updates from the manufacturer/service provider only.

The manufacturer/service provider shall maintain appropriate cyber security standards for the update process itself and the management of updates within the manufacturers', and partners', organizations.

The CEM local to the ESA shall receive software and firmware updates over a secure dedicated logical communications link with the manufacturer/service provider only. The secure communications link shall be set up using mutual authentication and shall allow messages to be encrypted (see **6.2**).

A remote CEM, based in the cloud, shall receive and install software updates from the CEM vendor or service provider according to industry best practice (depending upon the particular architecture or platform used), e.g. NCSC's *Cloud Security Principles* [N2]. The remote CEM shall only perform an update if the update originator is authenticated and the update image integrity is assured using hashing and signatures.

It shall not be possible for the Consumer or any other unauthorized party to perform software and firmware updates on the ESA or CEM that affect DSR services and functionality.

It shall not be possible for the Consumer or any other unauthorized party to pause or cancel any validated software and firmware updates on the ESA or CEM that correspond to cyber security functionality.

All software and firmware images shall be hashed, signed and encrypted before being sent to the ESA and local CEM.

The ESA and local CEM shall not install software and firmware updates if the update image does not pass an integrity check (via hashing/signature).

If an update image does not pass an integrity check then the ESA or CEM shall enter an "update image failed integrity check" event (including time) in its secure log.

The ESA and CEM shall securely store the version number of the software and firmware currently in use.

The ESA and CEM may securely store the version number of any non-active software and firmware currently stored.

The ESA and CEM shall be able to roll back to the most recent "known good" version.

Installation of firmware and software updates for a cohort of ESAs and CEMs shall not be performed at the same time.

Critical security software and firmware updates should be installed as soon as possible.

Software updates shall be installed by the remote CEM provider such that there is no interruption of CEM service provision.

The ESA and CEM shall not interrupt an active DSR event in order to perform an update installation.

6.11 Secure storage area

The CEM and ESA shall store security sensitive information in a secure, tamper-resistant, logically separate area that shall be compliant with NIST FIPS 140-2 Level 3.

It shall be possible for data stored in this secure area to be securely erased, meaning that the data shall no longer be present in the storage medium and shall not be accessible in any way.

The CEM and ESA shall incorporate a Security Log in this tamper-resistant area consisting of Coordinated Universal Time (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.

The CEM and ESA shall obtain UTC values using Network Time Security (NTS), as specified by RFC 8915.

The use of passwords is not recommended but passwords used to authenticate the Consumer 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 Consumer 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, timestamp). If the password is defined by the Consumer 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.).

The secure storage area shall include:

a) digital certificates;
b) keys;
c) a Security Event Log, which shall record:
    1) time stamped entries;
    2) accepted and rejected tests applied during mutual authentication processes (**5.3.2**);
    3) attempts to install unauthenticated software/ firmware;
    4) unauthorized attempts to access communications port;
    5) event type (i.e. messages sent, messages received and messages acted upon); and
    6) reception of unauthenticated messages;
d) the Operation Log, including acceptance of flexibility offer requests.

The Security Event Log and Operation Log shall each contain at least 100 entries and shall be circular buffers.

The ESA or CEM shall be capable of sending all or part of the contents of the secure storage area to authorized parties over an encrypted link using signed messages.

Authorized parties shall be limited to:

a) the Consumer, which shall have access to the Operation Log and the Security Event Log information via the CEM or ESA user interface;
b) the DSRSP, which shall be given access to the Operation Log and the Security Event Log information; and
c) the ESA and CEM manufacturer/service provider, which shall be given access to the Security Event Log.

6.12 Anomaly detection and data validation

The ESA/CEM shall only permit sending of flexibility information within its defined operating capability and limits; and where the message type is within its defined operating approach.

The ESA/CEM shall only allow acting on DSRSP flexibility messages where the content matches the ESA/CEM sent flexibility message and is within its defined operating capability and limits; and where the message type is within its defined operating approach.

The ESA/CEM shall monitor the number of messages sent, received and acted on over a time period. Where the number in a given time period exceeds appropriate thresholds, the ESA/CEM shall log these events (timestamp and event type) in its Security Events Log and provide this Log to the DSRSP in accordance with **6.11** and **6.13**; additionally the ESA/CEM shall enter a failsafe state (**5.3.5.2.5**) if appropriate.

6.13 Security incident management

6.13.1 Event logging and reporting

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.

Whenever a CEM or ESA detects:

a) a failure of tests conducted during the mutual authentication processes;

b) an attempt to access any of its communication interfaces or ports by an unauthorized party (no or incorrect encryption or signature);

c) an attempt to install unauthorized software/ firmware (incorrect hash or signature); or

d) reception of incorrectly signed or encrypted messages,

it shall log these events (timestamp and event type) in its Security Events Log.

The CEM or ESA shall provide the contents of its Security Events Log to the DSRSP upon request from the DSRSP or whenever a given threshold of events, or buffer occupancy, is reached.

***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.*

6.13.2 Vulnerability disclosure

ESA/CEM manufacturers shall disclose vulnerabilities in accordance with the vulnerability report management provisions included in EN 303 645.

6.14 Phases of operation

*COMMENTARY ON **6.14***

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

- *pre-requisites;*
- *authentication and registration;*
- *normal operation; and*
- *de-registration.*

6.14.1 Pre-requisites

6.14.1.1 Digital certificate 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** The functionality of registration authorities might or might not exist to grant approval to DSRSPs and CAs to operate as trusted entities in the DSR architecture. This optional functionality is at the discretion of any responsible national authorities for a specific geography. 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.*

6.14.1.2 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.

a) The ESA shall be connected to either the consumer home network or to a remote communications bearer such as a mobile data connection.

b) The local CEM, if present, shall be connected to the consumer home network or to a remote communications bearer such as a mobile data connection.

c) Where the ESA supports only a mobile data connection and requires connection to a local CEM, then the ESA shall always be allowed to connect to such a CEM (e.g. by configuration of the home gateway).

d) The local CEM and ESA, if connected to the consumer home network, shall be connected to their respective manufacturer or service provider portals via either the home network router or gateway.

e) The local CEM and ESA, if connected to a remote communications bearer, shall be connected to their respective manufacturer or service provider portals via that remote communications bearer.

f) The local CEM shall be mutually authenticated and registered with its manufacturer or service provider portal and the link between them shall be capable of transferring encrypted messages.

g) The ESA shall be mutually authenticated and registered with its manufacturer or service provider portal and the link between them shall be capable of transferring encrypted messages.

h) Any software, firmware or security credential updates shall be performed securely, using TLS v1.3 or later.

i) The CEM shall check with its manufacturer or service provider portal for manufacturer approved firmware/software updates and perform a secure update if a more recent version is available (see **6.10** for software and firmware updates).

j) The ESA shall check with its manufacturer or service provider portal for manufacturer approved firmware/software updates and perform a secure update if a more recent version is available (see **6.10** for software and firmware updates).

NOTE 1 *The CEM and ESA can optionally connect to a smart metering system network. Requirements for connectivity to the GB smart metering system are described in Annex **D**.*

NOTE 2 *Within the context of this PAS, the CEM and ESA are connected to their respective manufacturer or service provider portals for the purposes of registration, DSR function related software and firmware updates (including security updates) and DSR related configuration information (e.g. power profile table updates). It is recognized that these interfaces might also be used for non-DSR functionality (e.g. updates to operational capabilities).*

6.14.2 Authentication and registration

*COMMENTARY ON **6.14.2***

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 consumer registration;*
- *CEM and ESA mutual authentication; and*
- *DSRSP and CEM authentication and registration.*

6.14.2.1 DSRSP service consumer registration

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

a) CEM service provider name;

b) CEM manufacturer name; and

c) CEM serial number.

The consumer 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:

1) CEM service provider name;

2) CEM manufacturer name;

3) CEM serial number;

4) consumer electricity supplier; and

5) agreement to contract DSR services.

The consumer shall be provided with CEM registration URL as a minimum by th.e DSRSP (this URL is to be used during the CEM/ESA–DSRSP service authentication and registration processes)

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.*

6.14.2.2 CEM and ESA mutual authentication

*COMMENTARY ON **6.14.2.2***

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.

6.14.2.2.1 General requirements

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

a) The latest manufacturer approved CEM and ESA firmware and/or software versions shall be successfully installed prior to commencement of the authentication process. This shall be performed over the authenticated and encrypted link set up with the manufacturer or service provider, as described in **6.14.1.2**.

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 Consumer.

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 authentication, using TLS v1.3 or later.

i) Additional unambiguous identification methods shall be used as a second stage of authentication and shall make use of signatures and encrypted links.

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

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

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

***NOTE** The CEM can use the information provided by the ESA for device validation (e.g. firmware version validity, cross-reference of manufacturer and model) or operation validation (e.g. comparing flexibility offers with that expected of the ESA type). The CEM can pass the information to the DSRSP for similar such validation.*

6.14.2.2.2 CEM-ESA mutual authentication process

***NOTE 1** The ESA and CEM can be pre-provisioned with the information required for mutual authorization, for instance if they are provided by the manufacturer as a pair.*

a) The steps described in **6.14.2.1** shall be performed prior to CEM/ESA mutual authentication.

b) The ESA shall be placed into "CEM discovery mode" by the Consumer (DSRSP subscriber).

c) If a remote CEM is used:

1) the Consumer shall sign in to the CEM service portal;

2) the CEM service provider shall provide the Consumer with an ESA registration URL using the CEM service provider portal;

3) the ESA shall be provided with the ESA registration URL by the consumer; and

4) the ESA shall contact the ESA registration URL.

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

e) The CEM and the ESA shall mutually authenticate using TLS v1.3 or later.

f) If the CEM fails authentication with the ESA, then the ESA shall log the authentication fail event and inform the consumer via its user interface. No further authentication attempts shall be made by the ESA until instructed by the Consumer.

g) If the ESA fails authentication with the CEM, then the CEM shall log the authentication fail event and inform the Consumer via its user interface. No further authentication attempts with the particular ESA shall be made by the CEM until instructed by the Consumer.

h) If the mutual authentication is successful then both the CEM and ESA shall log the successful authentication event and inform the Consumer via their respective user interfaces.

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

j) The CEM and ESA shall then enter a second phase of authentication that is intended to prove that the Consumer is physically present with the ESA and to allow the Consumer to approve authentication. The details of this process shall be determined by the CEM and ESA manufacturer/service provider and shall meet the following requirements:

1) the process shall validate that the Consumer is physically present with the ESA;

2) the process shall ensure that the Consumer approves the authentication of the CEM and ESA;

3) the process shall minimize and simplify interaction with the Consumer as much as is feasible (in order to reduce the possibility of "user error"); and

4) interim use of a browser, application or other such channel running on a third device (e.g. mobile phone, tablet) during this phase shall be permitted.

k) Following successful authentication, the CEM shall add the ESA to its "allowed list".

l) The ESA shall send its manufacturer name, serial number, EUI-64 and firmware version in a signed message to the CEM over the encrypted link.

***NOTE 2** This information may be used by the CEM to identify the ESA and to validate the ESA software/ firmware version.*

m) If the CEM cannot verify the signature of the message, then it shall log the "ESA signature fail" event and notify the Consumer.

***NOTE 3** The manufacturer and serial no. info could also be used by the CEM to validate any subsequent flex offers from the ESA. For example if the CEM knows that the device is a washing machine, but it starts seeing flex offers offering 7kW of flex, then there is clearly something amiss. This information could also be passed to the DSRSP for similar validation.*

***NOTE 4** The CEM can verify the ESA model and firmware version using a 3rd party connection.*

6.14.2.3 DSRSP and CEM authentication and registration

The DSRSP and CEM shall mutually authenticate using the following process.

a) The steps described in **6.14.2.1** shall be performed prior to DSRSP/CEM mutual authentication.

b) Prior to DSRSP/CEM mutual authentication, the Consumer shall have successfully signed up to a DSRSP and requested to register a CEM with the DSRSP.

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

c) The DSRSP shall be able to provide the Consumer with a CEM registration URL.

d) The Consumer shall 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.*

e) The CEM shall contact the DSRSP using the CEM registration URL.

NOTE 3 *One-way authentication maybe used for this connection (e.g. HTTPS).*

f) The CEM and DSRSP shall mutually authenticate using TLS v1.3 or later.

g) If the CEM fails authentication with the DSRSP, or the DSRSP fails the authentication attempt with the CEM, then the CEM shall log the authentication fail event and inform the Consumer via its user interface. No further authentication attempts shall be made by the CEM until instructed by the Consumer.

h) If the mutual authentication is successful then the CEM shall log the successful authentication event and inform the consumer via its user interface.

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

j) The DSRSP and CEM shall then enter a second phase of authentication that is intended to allow the Consumer to approve authentication. The details of this process shall be determined by the CEM and ESA manufacturer/service provider and shall meet the following requirements:

   1) the process shall ensure that the Consumer approves the authentication of the DSRSP and CEM;

   2) the process shall minimize and simplify interaction with the Consumer as much as is feasible (in order to reduce the possibility of "user error");

   3) interim use of a browser, application or other such channel running on a third device (e.g. mobile phone, tablet) during this phase shall be permitted.

k) The CEM shall send its manufacturer, serial number, EUI-64 and firmware version in a signed message to the DSRSP over the encrypted link.

NOTE 4 *This information may be used by the CEM to identify the ESA and to validate the ESA software/ firmware version.*

NOTE 5 *The DSRSP might be able to verify the integrity of the message by verifying the signature. The DSRSP might also be able to verify the CEM model and firmware version using a third party service connection.*

l) If the CEM verification is successful then the CEM shall add the DSRSP to its "allowed list". The DSRSP shall be able to add the CEM EUI-64 to its CEM Allowed List.

m) If already obtained through the CEM and ESA mutual authentication process, the CEM shall send the ESA manufacturer name, serial number, EUI-64 and firmware version in a signed message to the DSRSP over the encrypted link.

NOTE 6 *The DSRSP may be able to verify the ESA model and firmware version using a 3rd party connection.*

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

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

6.14.3 Operation phase

6.14.3.1 General

In normal operation, messages shall be sent securely over Interface A between the DSRSP and CEM and over Interface B between the CEM and ESA.

Components shall only accept and act upon DSR related messages received from other components with which they have registered (with the exception of during the registration phase).

Components shall only send DSR related messages to other components with which they have registered (with the exception of during the registration phase).

All messages in the operation phase shall 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 shall be encrypted to ensure data privacy and cyber security.

6.14.3.2 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 be encrypted and signed by the CEM and shall include:

a) ESA and CEM information used during the authentication and registration phases;
b) ESA flexibility offers and forecast updates;
c) ESA status information;
d) certificate update notification and new certificates;
e) ESA or CEM originated de-registration notification; and
f) notification of tampering or attempted tampering of the CEM or ESA.

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

1) information sent by the DSRSP during the CEM and ESA authentication and registration processes;
2) requests for ESA status updates;
3) ESA flexibility offer selection messages;
4) DSRSP originated CEM or ESA de-registration notification; and
5) certificate update notification and new certificates.

6.14.3.3 Interface B messages

Messages sent over Interface B shall conform to any security requirements in the implemented interface protocol. The messages sent across Interface B shall include the following and shall be subject to the encryption and signature rules denoted.

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

6.14.4 De-registration

*COMMENTARY ON **6.14.4***

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

A CEM and ESA shall be registered to only one DSRSP at any given time. A CEM or ESA shall de-register with its existing DSRSP before registering with a new 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 (e.g. DSRSP URL, DSRSP certificate) and shall request the DSRSP to delete (remove) any information stored that is associated with the CEM, ESA or consumer. A de-registered CEM or ESA shall be able to re-join the DSRSP service only through the registration process described in **6.14.2**.

A consumer shall request that a CEM or ESA is de-registered by first contacting the DSRSP. The subsequent process is broadly determined by the DSRSP but, at a minimum, the associated CEM or ESA shall subsequently

receive a "de-registration" message from the DSRSP. The CEM or ESA shall inform the Consumer via its user interface that a de-registration request is in progress. The Consumer shall accept or decline the request via the CEM or ESA user interface. If accepted, the CEM or ESA shall send a signed "de-registration acknowledge" message to the DSRSP (signed by the DSRSP and interpreted by the CEM). Any communication across Interface A and Interface B shall make use of the PKI and encryption set up in **6.14.1.1** and **6.14.2.2.1**. The CEM or ESA shall then cease all DSR related operations and remove the DSRSP from its "allowed list".

NOTE 1 *The DSRSP may remove the CEM or ESA from its list of active devices and from its "allowed list".*

NOTE 2 *A DSRSP should inform the consumer that a CEM or ESA is being de-registered before the de-registration process is initiated. The Consumer then has the opportunity to accept or decline the de-registration.*

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 beyond 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 shall not be prevented from connecting to a different CEM to the one with which it was originally supplied, provided the requirements in Clause **6** are met.

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 and external information (when available) as necessary.

The CEM and ESA shall operate according to the four operating modes specified in **5.3.5.2**.

The CEM and ESA shall use the operating mode priority ordering specified in **5.3.5.3**.

ESA manufacturers and service providers shall ensure there are sufficient consumer support channels, and ESAs are clearly labelled with the manufacturer and at least one route of consumer contact, i.e. a website, phone number, email, etc. for consumers to use when in need of support.

7.2 Start up and shut down

7.2.1 Start up

When starting up (when links have already been authenticated) or coming out of standby, the ESA or CEM shall re-connect to its network(s).

The ESA shall provide a flexibility offer to the DSRSP, via the CEM, according to the security mechanisms described in **6.13**.

7.2.2 Shut down

If the ESA is able to gracefully shut down (i.e. not as a consequence of a power or communications failure) then the ESA shall send to the DSRSP a flexibility offer consisting of a single "zero" power forecast profile for each profile type.

If the ESA or CEM is not able to shut down in a graceful manner (e.g. power loss) then it shall behave according to **5.3.5.2.5**.

7.3 ESA architecture

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

***NOTE 1** The physical layer is not specified.*

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 with no loss or corruption of information.

The CEM might have the capability to connect to more than one ESA at any given time.

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 direct measurement or some other means and according to **5.6**.

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

NOTE 3 *The ESA can incorporate one or more additional interfaces, as denoted in Figure 4. Except for security requirements, such interfaces are beyond the scope of this PAS, although example uses include remote maintenance and remote selection of programmes by the consumer.*

7.4 Consumer action

The ESA shall include a local (built in) and/or remote (for example on a smart phone application) user interface.

NOTE *The CEM might include a local (built in) and/or remote (for example on a smart phone application) user interface.*

The ESA user interface shall provide at least the following:

a) current and planned power consumption;
b) DSR mode enable/disable;
c) DSR status (DSR event in progress, not in progress, planned DSR operation);
d) DSR event cancel (required on ESA only and optional on the CEM);
e) input of communications credentials sufficient to allow the device to connect to a network (e.g. SSID, WiFi password);
f) input of registration and authentication credentials (depends upon cyber-security requirements); and
g) consumer preferences (e.g. for the configuration of notifications and the user interface or of an accessible user interface).

NOTE *The ESA 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.*

Interaction with the ESA user interface (either integrated or remote) shall take precedence over any previous interaction with other devices (e.g. CEM).

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

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

If the ESA includes integrated CEM functionality then it the ESA user interface shall allow the CEM functionality to be disabled in order to allow the ESA to connect to a different CEM.

7.5 Installation and initiation

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

Installation and initialization of the energy smart functionality of an ESA 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.

The ESA and CEM shall perform network connection upon instigation by the Consumer and shall connect to their respective manufacture/service provider portals according to **6.14.1.2**.

The ESA and CEM shall mutually authenticate and authenticate with the DSRSP according to **6.14.2.2**.

Following authentication, the ESA shall exchange information with the DSRSP, via the CEM, concerning its flexibility capabilities as described in **5.4.4**.

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

As part of its user interface, the ESA and CEM shall incorporate an indicator showing the status of each communication link. The indicator shall at least indicate that the link is operating or not. The indicator shall relate to both the physical and logical links combined.

7.6 General operation

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

7.7 Safety

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

7.8 Power value or profile provision

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

7.9 Loss of communication

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, via the CEM, 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.*

If the DSRSP has included a timeout value in 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).

NOTE 2 *If the CEM indicates that it is capable of storing power information, the ESA might send instantaneous power values or power profiles to the CEM for later transmission to the DSRSP.*

In the case of exception conditions the ESA shall transition or reset to a mode that brings it into a safe state as described in **5.3.5.2.5**. The ESA shall report its change in flexibility status to the DSRSP whenever possible.

NOTE 3 *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 CEM and DSRSP and initialize its flexibility status within 10 min.

7.10 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.

The UTC time reference shall be obtained using NTS, as specified by RFC 8915.

If the flexibility offer request is actioned by the DSRSP, the ESA shall begin flexibility operations within 1 s of the time specified in the flexibility offer.

The ESA shall send a flexibility offer update message to its CEM in order to notify it of any change in flexibility capability within 5 s of the ESA moving to a new flexibility state.

The CEM shall send a message to its DSRSP in order to notify it of any change in the flexibility capability of the ESA within 5 s of receiving a flexibility offer update message from the ESA.

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

NOTE *Routine method 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.*

7.11 Optional frequency-based services

If they have the capability, ESAs shall perform frequency-based services as described in **5.5.5**. These services may range from long-duration, despatched response through to short-duration, autonomous response for improving the stability of the electricity system.

7.12 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 Security Event Log as described in **6.11**.

An ESA shall operate according to **6.13** if it detects a tamper attempt.

7.13 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 Response DSR services.*

Consumers shall have appropriate rights over the 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 **7.14**.

7.14 Cyber security

Key pair generation and private key storage shall be performed as described in **6.4**.

A CEM/ESA shall conform to EN 303 645 and to Clause **6**.

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

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

A CEM/ESA shall not include any enabled physical interfaces not used in its normal operation (e.g. JTAG port).

CEM/ESA firmware shall be protected, and firmware updates shall be made secure, as described in **6.10**.

Data held by CEMs/ESAs shall be protected, as described in **6.6**.

Any passwords, identifiers and other security related data stored on the ESA or CEM (with the exception of certificates and shared keys generated during the authentication process) shall be unique.

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

7.15 Lifecycle

The contents of the ESA and CEM secure storage area shall be erased upon de-commissioning.

8 Specific ESA requirements

8.1 Smart EV chargepoint

The smart EV chargepoint ESA shall be capable of reporting forecast power profiles based on operating capabilities, consumer preferences, including expected departure/arrival schedule and journey distance/duration/characteristics, and external information, including estimates of EV battery capacity, EV state of charge and EV physical operating limits. 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** and Clause **6**.

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

A.1 Set-up type use cases

A.1.1 ESA registration and set-up (consumer installation, first turn on)

A.1.1.1 Aim

a) The ESA is authenticated to DSRSP and to any relevant intermediate components.
b) The ESA is able to exchange energy flexibility messages with DSRSP and relevant intermediate components.

A.1.1.2 Assumptions

The ESA is installed by the consumer.

A.1.1.3 Pre-conditions

a) The ESA is in situ in consumer premises.
b) Consumer HAN is operational.
c) DSRSP WAN is operational.

A.1.1.4 Actors and components

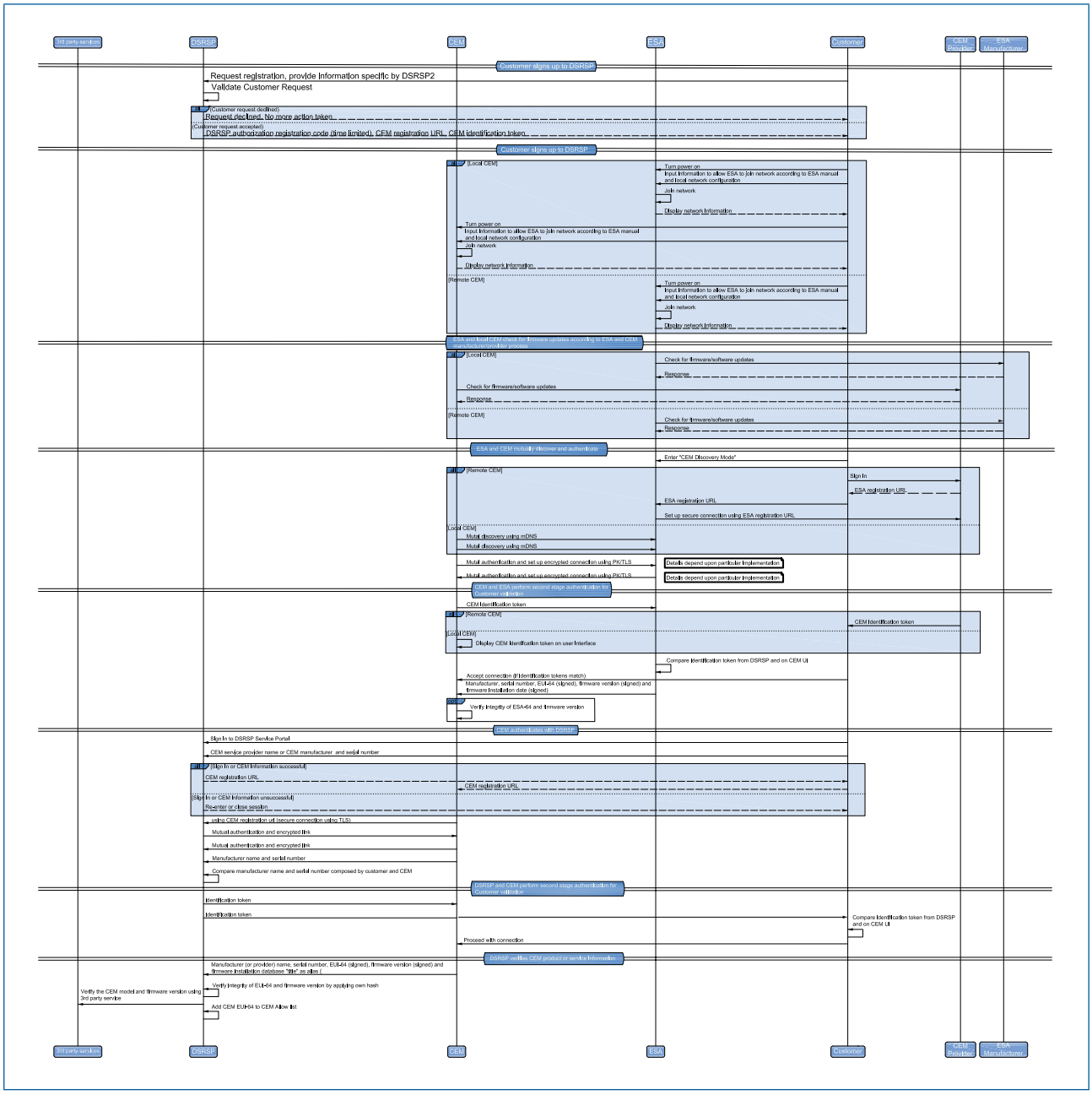
a) DSRSP
b) Consumer
c) ESA
d) CEM

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:

a) Consumer registers with DSRSP and receives time limited registration information to provide to the ESA and/or CEM (using a process defined by the DSRSP);
b) Consumer joins the ESA and the local CEM to the (local) network (no action is required for a remote CEM);
c) the ESA and local CEM perform firmware updates as required;
d) the ESA and CEM mutually discover and authenticate using best practice methods;
e) the ESA and CEM perform a secondary authentication procedure requiring Consumer approval;
f) the CEM adds the ESA to its "Allowed list";
g) Consumer 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 Consumer provides to the CEM (using a CEM specific process);
h) the CEM and DSRSP mutually authenticate using best practice methods;
i) the CEM and DSRSP perform a secondary authentication procedure requiring Consumer approval; and
j) the DSRSP adds the CEM to its "CEM Allowed 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 the 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

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

A.1.2.4 Actors and components

a) DSRSP
b) Consumer
c) ESA
d) 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.2.

a) Customer contacts the incumbent DSRSP and requests de-registration of an ESA and CEM;
b) Customer enters "de-register DSRSP" mode in both the CEM;
c) the CEM sends a "de-registration" message to the DSRSP;
d) the DSRSP validates the de-registration message and contacts Customer for validation of the de-registration;
e) 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;
f) the CEM and ESA remove all appropriate DSRSP information from their storage; and
g) the registration process described in **A.1.1.5** is invoked by the Customer to register with a new DSRSP.

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

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

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

A.1.3.4 Actors and components

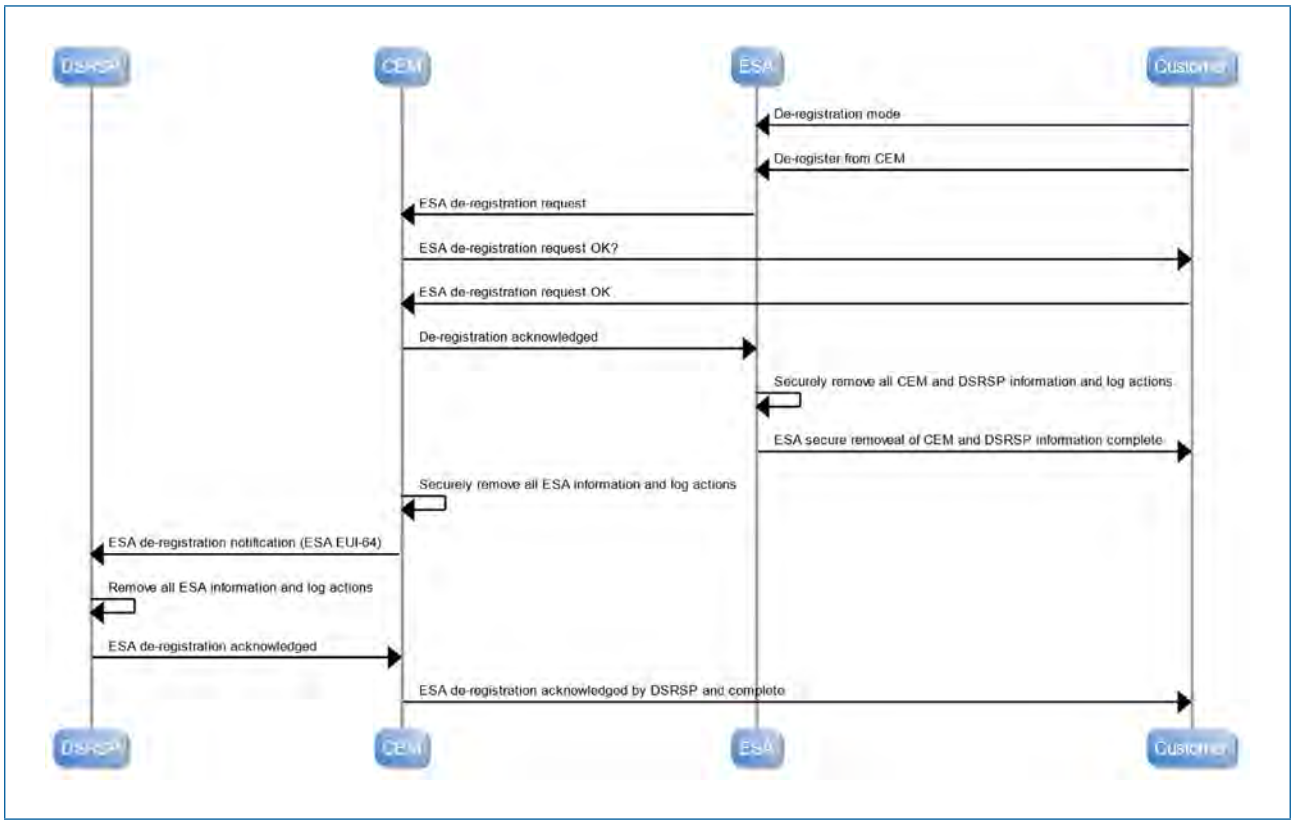
a) DSRSP
b) Consumer
c) ESA
d) CEM

A.1.3.5 Sequence

An example sequence of interactions required for ESA de-registration is depicted in Figure A.3 and may be summarized as:

a) Consumer places the ESA into de-registration mode;
b) Consumer selects "de-register from CEM";
c) the ESA sends a de-registration request to the CEM;
d) the CEM waits for confirmation of ESA de-registration from the Consumer (via the CEM UI);
e) the Consumer confirms the ESA de-registration to the CEM;
f) the CEM sends a "de-registration confirmed" message to the ESA;
g) the ESA securely removes all information related to the CEM and DSRSP, logging all actions;
h) the ESA informs the Consumer that it securely removed all CEM and DSRSP information;
i) the CEM securely removes all information related to the CEM and DSRSP, logging all actions;
j) the CEM sends an "ESA de-registration notification" message to the DSRSP;
k) the DSRSP securely removes all information related to the ESA and logs all actions;
l) the DSRSP sends an "ESA de-registration acknowledged" message to the CEM; and
m) the CEM informs the Consumer that the ESA de-registration process is complete and that ESA information has been removed from the DSRSP.

Figure A.2 – ESA is de-registered from CEM and DSRSP



A.2 Operation type use cases

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

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

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

A.2.1.4 Actors and components

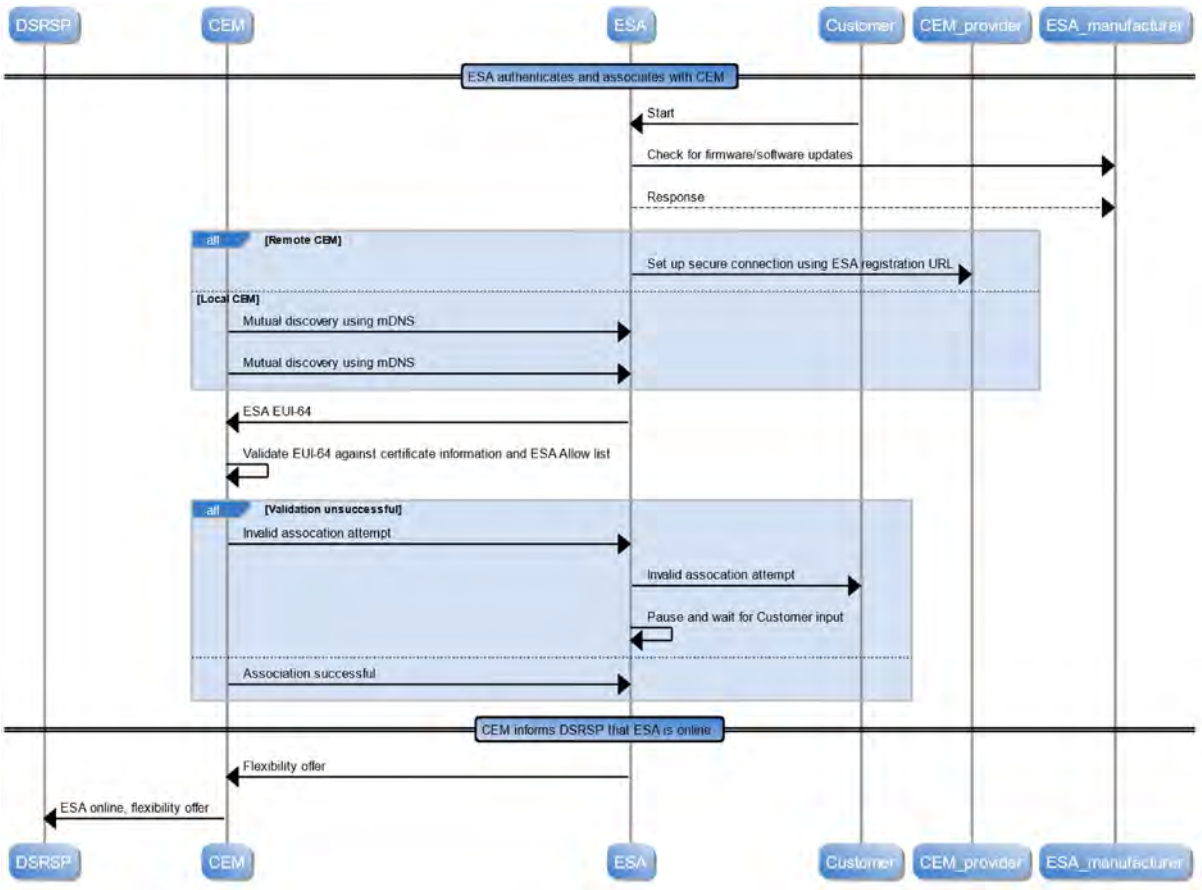
a) DSRSP
b) ESA
c) CEM

A.2.1.5 Sequence

An example sequence is depicted in Figure A.3.
The main steps are:

a) Consumer starts the ESA;
b) the ESA checks for firmware update;
c) the ESA and CEM mutually identify and authenticate (using best practice methods);
d) the CEM further validates the ESA against ESA information already stored in the ESA Allowed list;
e) the ESA passes flexibility offers to the CEM; and
f) the CEM informs the DSRSP that the ESA is back online and forwards the ESA flexibility offer.

Figure A.3 – ESA power-up (non-first turn on)



A.2.2 CEM responds to a DSRSP flexibility request (single ESA)

A.2.2.1 Aim

The ESA successfully executes a DSRSP energy flexibility request.

A.2.2.2 Assumptions

a) The ESA has the capability to report its own power consumption or production, either as periodic instantaneous measurements or as an actual power profile.
b) The ESA has the capability to provide at least three forecast power profiles.
c) The ESA maintains a secure "flexibility actions" log.
d) The CEM maintains a secure "flexibility actions" log.

A.2.2.3 Pre-conditions

a) The ESA is installed in premises and subscribed to a DSRSP energy flexibility service.
b) Consumer HAN is operational.
c) DSRSP WAN is operational.

A.2.2.4 Actors and components

a) DSRSP
b) Consumer
c) ESA
d) CEM

A.2.2.5 Sequence

An example sequence is listed below and depicted in Figure A.4.

a) The ESA sends its flexibility offers to the DSRSP via the CEM;
b) the CEM receives an "execute flexibility" request from the DSRSP, containing the proposed power profile;
c) the CEM acknowledges the "execute flexibility" request with the DSRSP;
d) The CEM requests the ESA to implement its flexibility offer;
e) the ESA executes the selected flexibility offer;
f) the ESA measures or calculates 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;
g) 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;
h) the CEM acknowledges the "flexibility request completed" message;
i) the ESA updates its flexibility actions log and returns to Routine state;
j) 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;
k) the DSRSP validates the "flexibility request completed" message and, if acceptable, acknowledges the "flexibility request completed" message;
    1) otherwise, the DSRSP sends a "flexibility request not acknowledged" message to the CEM;
    2) the CEM updates its flexibility actions log according to the DSRSP response;
l) the DSRSP updates the consumer's flexibility account accordingly; and
m) optionally, the DSRSP sends a message to the consumer, informing them of their recent flexibility contribution (perhaps including consumption or financial information).

Figure A.4 – ESA responds to DSRSP flexibility offer request

A.2.3 ESA modifies current ongoing flexibility forecast

A.2.3.1 Aim

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

A.2.3.2 Assumptions

None.

A.2.3.3 Pre-conditions

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

b) An ESA's flexibility offers change 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.2.3.4 Actors and components

a) DSRSP
b) Consumer
c) ESA
d) CEM
e) ESAG (if present)

A.2.3.5 Sequence

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

a) The status of the ESA changes and its current set of flexibility offers is no longer valid;
b) 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;
c) the ESA calculates a new set of flexibility offers and sends them to the CEM, indicating if the current flexibility offer is still valid or not;
d) the ESA continues to measure its power consumption or production;
e) the CEM passes the new set of flexibility offers to the DSRSP;
f) the DSRSP updates the active flexibility offers for the ESA and its records for the ESA; and
g) 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.

A.2.4 CEM operates multiple ESAs

A.2.4.1 Aim

The CEM manages energy flexibility across two or more ESAs.

A.2.4.2 Assumptions

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

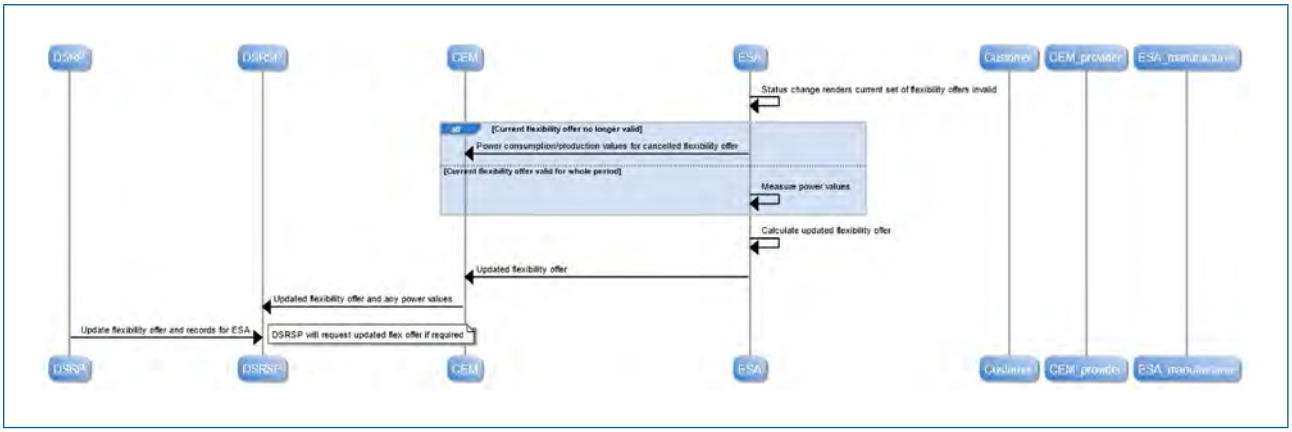
A.2.4.3 Pre-conditions

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

A.2.4.4 Actors and components

a) DSRSP
b) Consumer
c) ESA#1; ESA #2
d) CEM

Figure A.5 – ESA flexibility offer update



A.2.4.5 Sequence

Two example options for sequencing with multiple ESAs are depicted in Figure A.6 and Figure A.7.

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 disaggregates 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.6 – Multiple ESAs connected to one CEM – non-aggregated

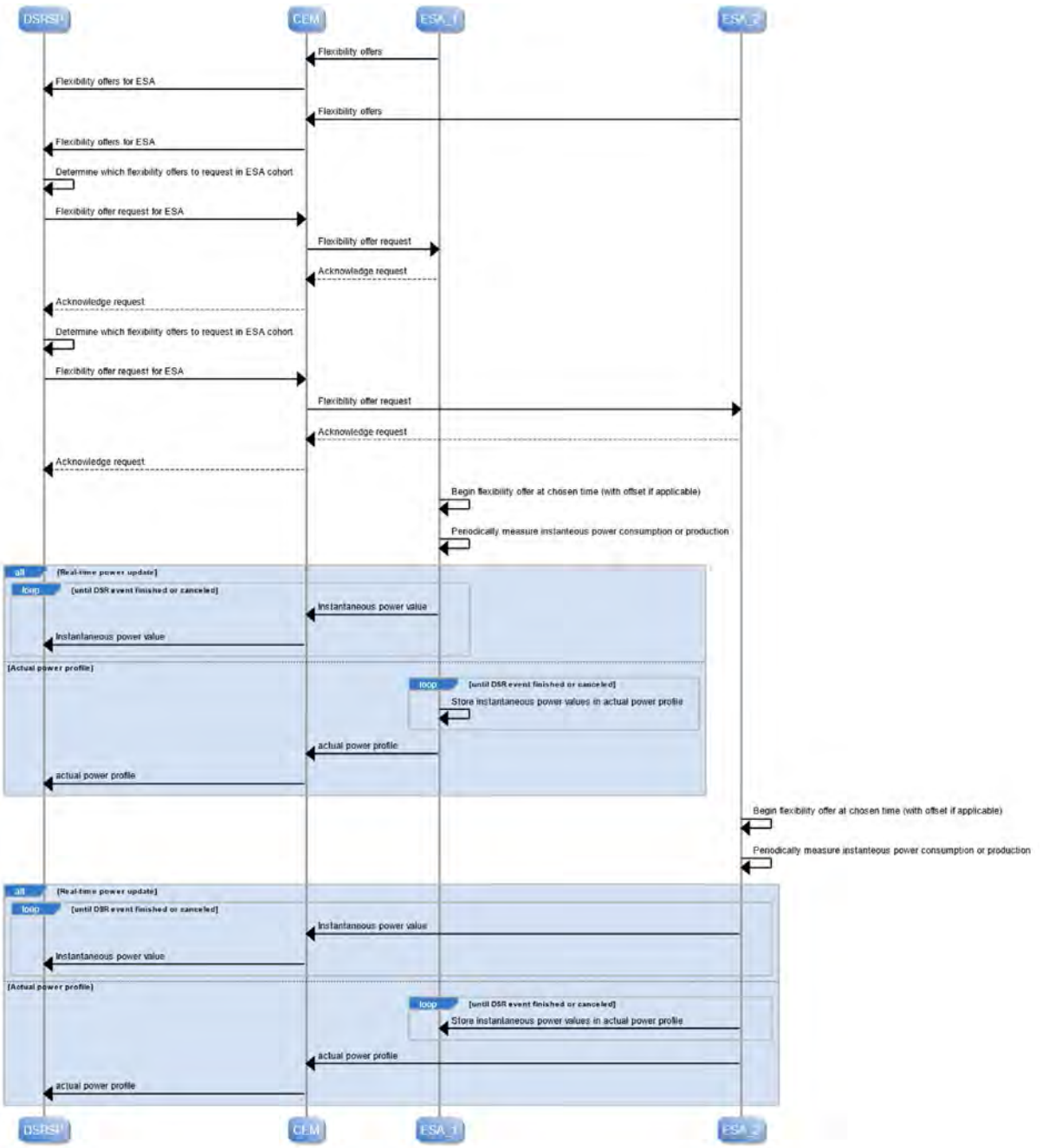
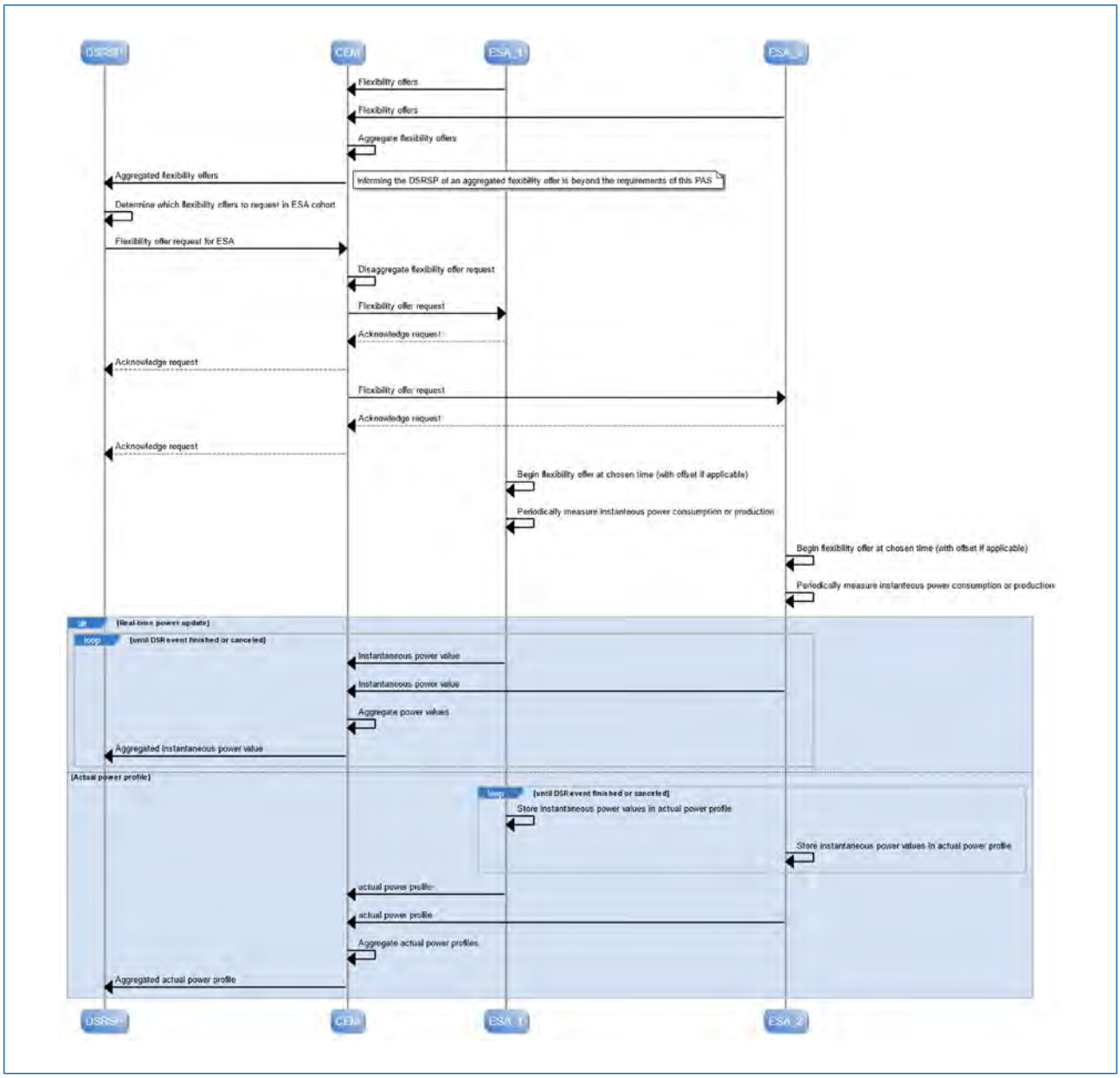


Figure A.7 – Multiple ESAs connected to one CEM – aggregated



A.3 Specific grid scenario type use cases

A.3.1 ESA and CEM recover from a loss of power to the premises

A.3.1.1 Aim

a) The ESA and CEM re-connect to the DSRSP after a power loss.

b) The ESA is once more able to exchange energy flexibility messages with the DSRSP and relevant intermediate components.

A.3.1.2 Assumptions

a) All components activate their smart interfaces upon power up.

b) All keys and related authentication and encryption information are securely stored on the component.

A.3.1.3 Pre-conditions

The ESA and CEM are already authenticated and operating with a DSRSP.

A.3.1.4 Actors and components

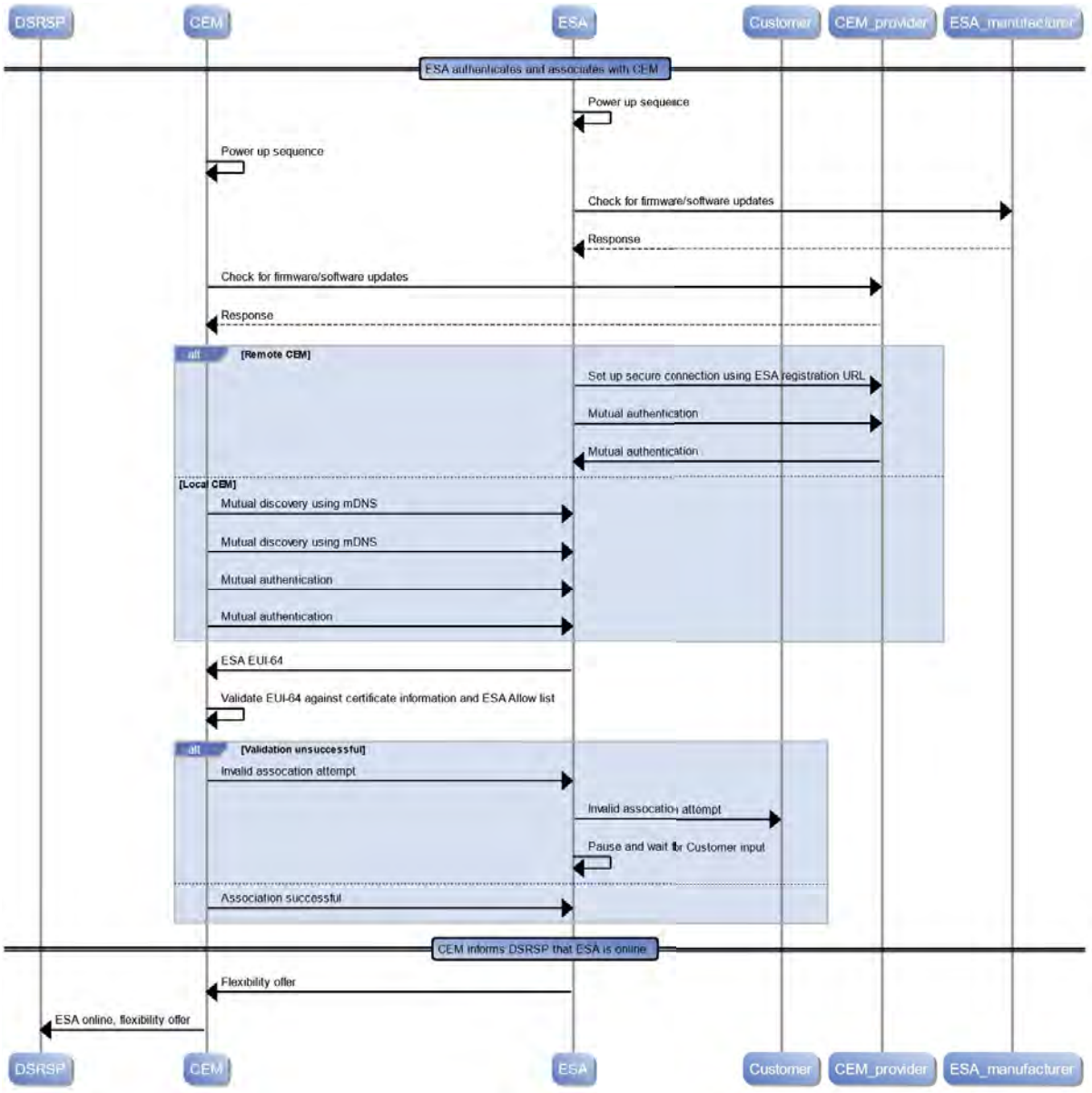
a) DSRSP
b) Consumer
c) ESA
d) CEM

A.3.1.5 Sequence

An example sequence is depicted in Figure A.8. The main steps are:

a) the ESA powers up;
b) the ESA checks for firmware update;
c) the CEM powers up;
d) the CEM checks for firmware update;
e) the ESA and CEM mutually identify and authenticate (using best practice methods);
f) the CEM further validates the ESA against ESA information already stored in the ESA Allowed list;
g) the ESA passes flexibility offers to the CEM; and
h) the CEM informs the DSRSP that the ESA is back online and forwards the ESA flexibility offer.

Figure A.8 – 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.

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.

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

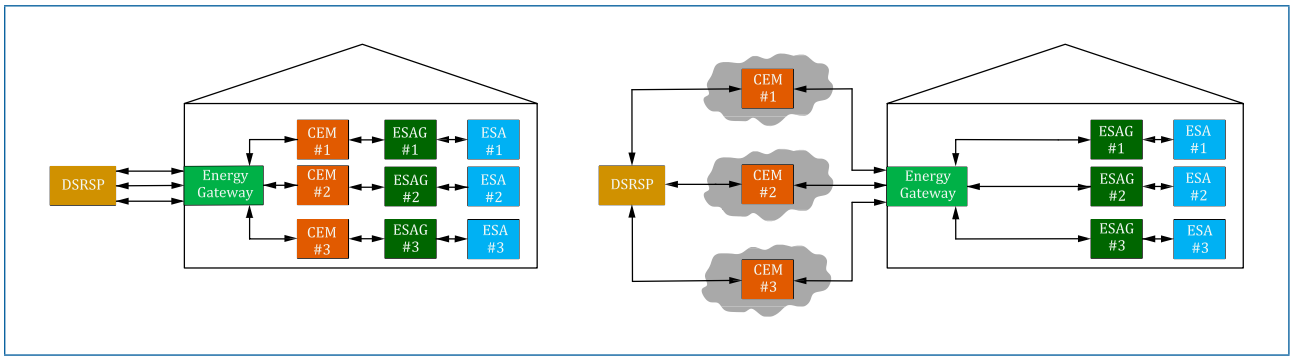
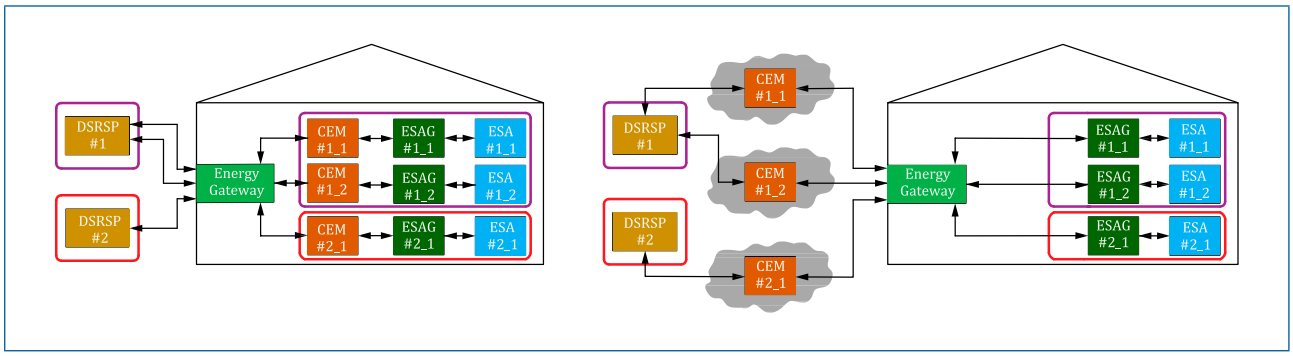


Figure B.2 – Multiple DSRSPs each controlling their own set of ESAs in a premises



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**.

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.

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

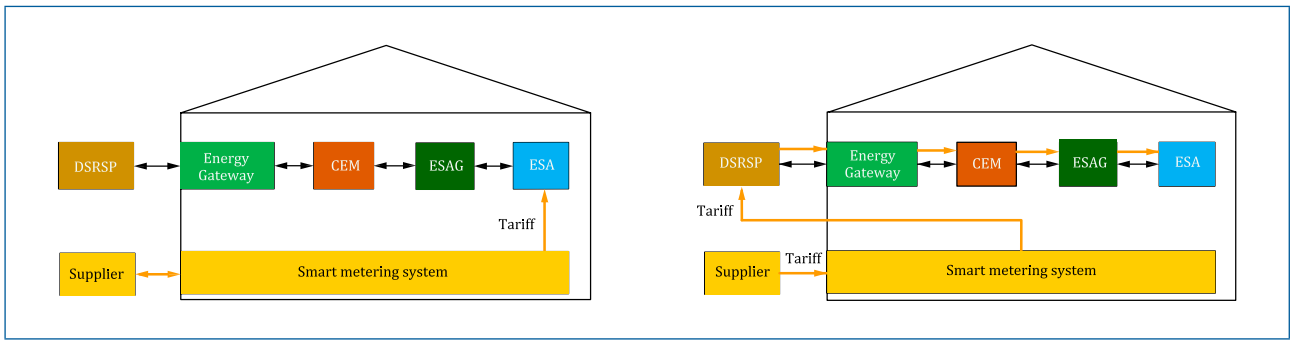
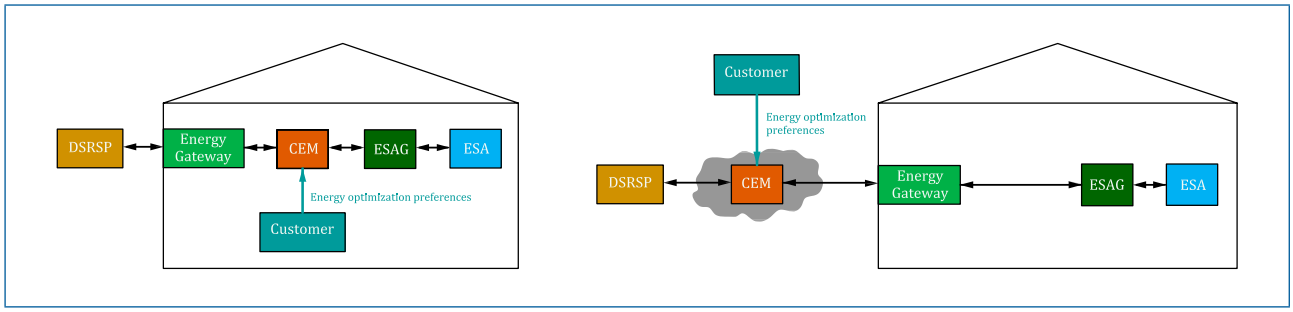


Figure B.4 – ESA operation in routine mode according to user preference optimization is superseded by response mode



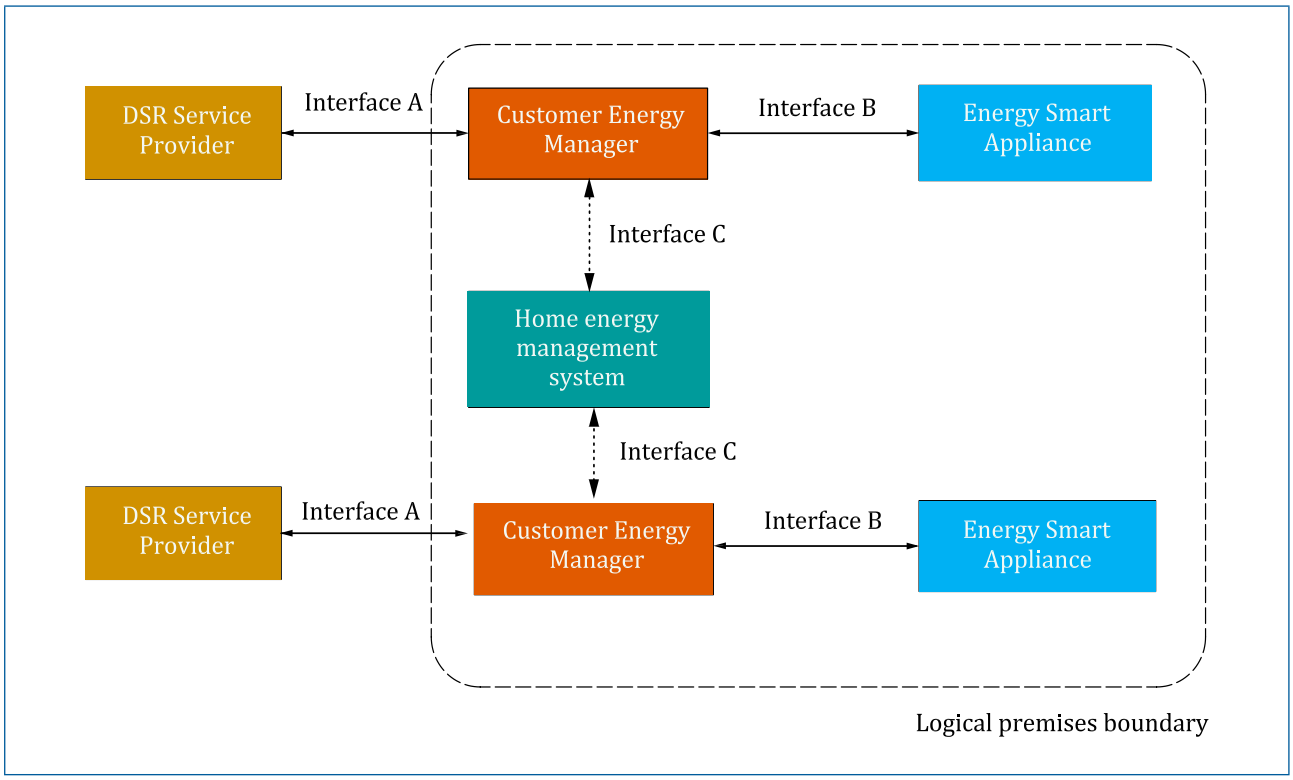
B.4 Routine mode using consumer preference optimization is superseded by response mode

Figure B.4 shows examples of how the consumer 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.

B.5 Multiple CEMs associated with a single premises connect to a single HEMS

Figure B.5 depicts how multiple ESA and/or premises level energy management may be carried out using a HEMS connected to multiple CEMs, where each CEM is connected to a single ESA.

Figure B.5 – Multiple and/or premises level energy management using "single ESA" CEMs and a HEMS



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 Table C.1, Table C.2, Table C.3, Table C.4).

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 chargepoints	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[9]. Tables C.3 and C.4 list minimum and maximum power classification options as an illustration of typical ESA power values which could be aggregated to provide DSR services.

[9] 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
Short Term Operating Reserve (STOR)		20 min to 240 min	≥120 min Recovery period <1200 min	A
Non-dynamic (static) Firm Frequency Response (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) Enhanced Frequency Response (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)]	Minimum power classifier
kW	
<(–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)]	Maximum power classifier
kW	
≤(–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 [8], GBCS [9] and DCC User Interface Specification [10];*
- *Technical and Business Architecture Documents [11];*
- *DCC User roles [12]; and*
- *Security and privacy obligations overview [13].*

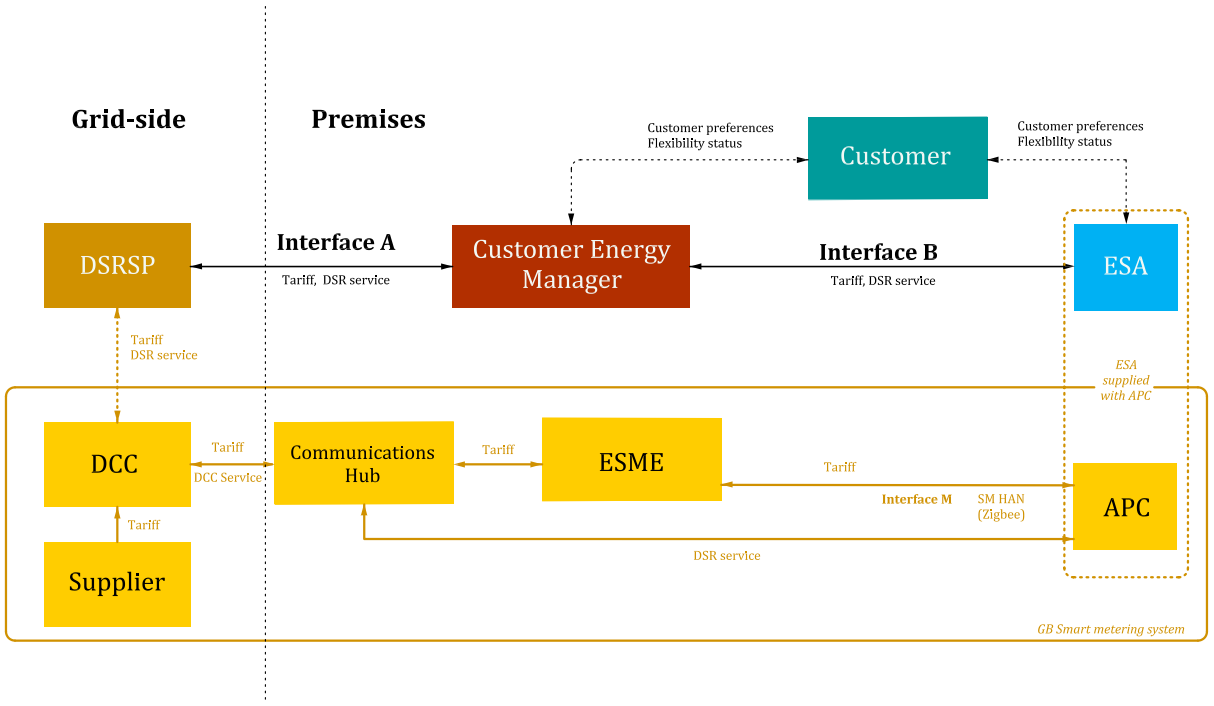
D.2 Architecture overview

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.

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



***NOTE** This is an example configuration, which shows an on-premises CEM. However, the CEM is a logical entity and may be sited outside the premises (i.e. cloud based). See Clause 4 for CEM configuration options.*

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

For tariff information access the following routes are possible:

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

For load control functionality the following routes are possible:

1) Route 3: load control over the smart metering network, via the APC;
2) 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.

a) Routes 1, 2, 3 and 4 require a CEM/ESAG in order to transmit power profile options created by the ESA from consumer preferences, external data and appliance information.
b) Routes 1 and 2 are the only routes which require an ESME.
c) Routes 1, 2 and 3 require a communications hub.
d) Route 3 is the only route which requires an APC, which is instantiated in an ESME or a SAPC.
e) Routes 1 and 3 require the ESA to be paired to the SMHAN and joined to the ESME by a DCC user.
f) Routes 2 and 3 require the DSRSP to be a DCC user in the user role of "Import Supplier".

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 **3.1.11** and **3.1.12**, a DSRSP operates ESAs, in line with consumer wishes, to provide DSR services to regulated electricity market participants. 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.

***NOTE** In the United Kingdom, import suppliers are registered against supply points via the Meter Point Administration Number (MPAN). If a premises is to support multiple import suppliers then multiple MPANs are required for that premises.*

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 Specification [14]. Its principal functions are:

a) acting as an interface between the DCC WAN and SMHAN;
b) acting as the SMHAN coordinator; and
c) providing a store of GSME data.

D.2.2.5 ESME

The ESME is a device described by the Smart Metering Equipment Technical Specifications [15]. Its principal functional areas are:

a) metering;
b) credit and prepayment payment modes;
c) ToU and block tariffs;
d) network monitoring; and
e) storage of consumption data.

D.2.2.6 Auxiliary proportional controller (APC)

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

a) the Import Supplier can set an output level of 0 to 100 in 0.1 increments;
b) the APC can provide event driven information ("alerts") to the Import Supplier about a load to which it is connected (for example power profile information);
c) the Import Supplier can set information on the APC about the load to which the APC is connected (via a number that can be interpreted as a reference to a power profile. Outside of this PAS the number could also be interpreted in other ways, for example as a percentage increase or decrease of consumption); and
d) 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 and SAPCTS version 5 [5] 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 ESA and the CEM/ESAG. The smart metering system can be used to deliver this information in two configurations:

a) Route 1: tariff over the SMHAN, via the ESA; or
b) 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), 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.

a) The tariff information is set on the ESME by the supplier.
b) The supplier passes tariff information for a consumer to the DCC.
c) The DCC routes the tariff information to the ESME, via the communications hub and SMHAN, in the consumer's premises.
d) The tariff information is made available over the SMHAN and the ESA supports a Zigbee SE interface to read this information.
e) The ESA passes the tariff information to the CEM/ESAG, via Interface B, if necessary.
f) The ESA uses the tariff information to create power profiles for routine and response mode operation, which are then passed, via the CEM/ESAG to the DSRSP.

The requirements for power profiles and updates are set out in **5.5** and **5.6**.

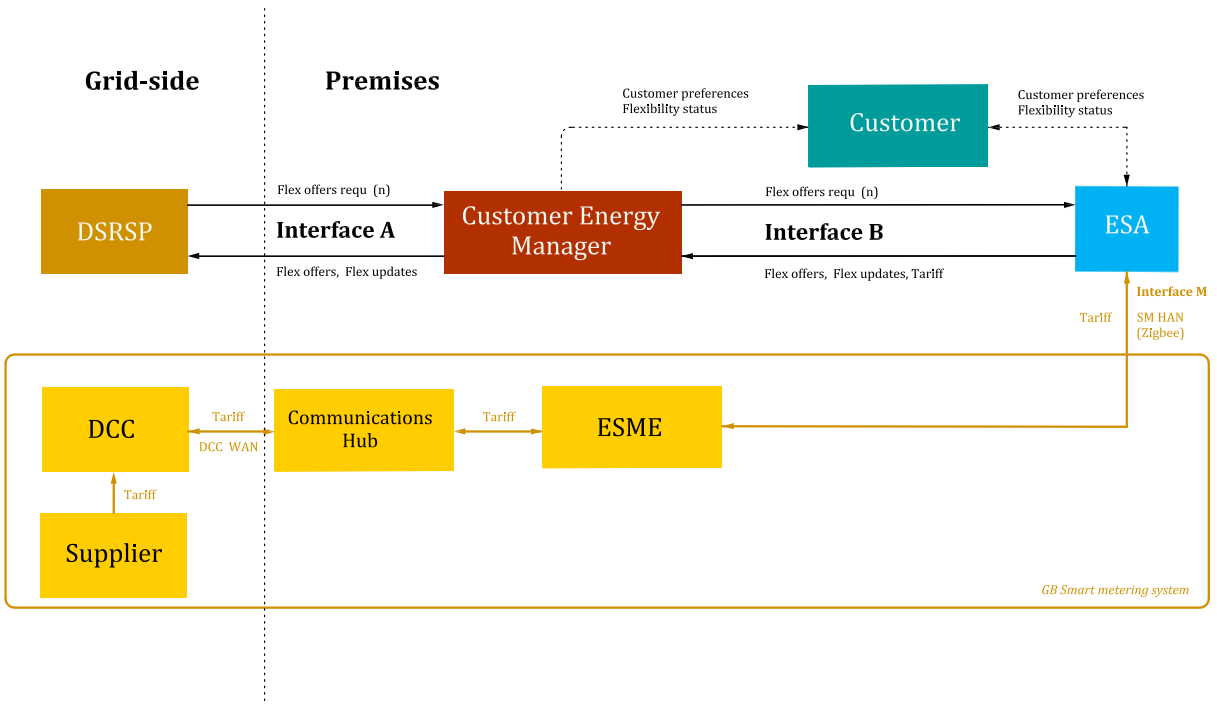
D.3.2.2 Summary of requirements

The main requirements for Route 1 are summarized below.

a) In order to support this configuration, the ESA incorporates a Zigbee Smart Energy interface – the so-called "Interface M". 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.).
b) A CEM/ESAG is used to transmit power profile options created by the ESA from consumer preferences, external data and appliance information.

NOTE *The system architecture for this configuration is shown in Figure D.2.*

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



***NOTE** This is an example configuration, which shows an on-premises CEM. However, the CEM is a logical entity and may be sited outside the premises (i.e. cloud based). See Clause **4** for CEM configuration options.*

D.3.3 Route 2: Tariff information via DCC WAN

D.3.3.1 Process flow

The process flow is as follows.

a) The tariff information is set on the ESME by the supplier.

b) The Supplier passes tariff information for a consumer to the DCC.

c) The DCC routes the tariff information to the ESME, via the communications hub and SMHAN, in the consumer's premises.

d) The tariff information is read from the ESME by the DSRSP, via the communications hub and the DCC.

e) The DSRSP passes the tariff information to the CEM/ESAG, via the S1 interface, and the ESA is internet enabled to read this information.

f) The ESA use the tariff information to create power profiles for routine and response mode operation, which are then passed, via the CEM/ESAG, to the DSRSP.

The requirements for power profiles and updates are set out in **5.5** and **5.6**.

D.3.3.2 Summary of requirements

The main requirements for Route 2 are summarized below.

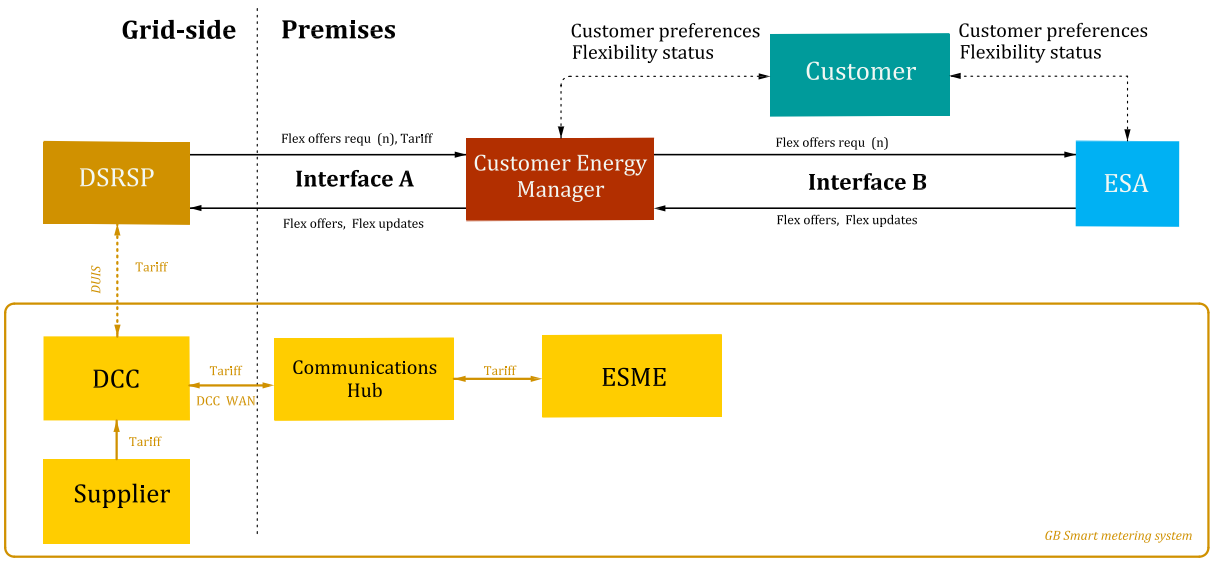
a) In order to support this configuration, the DSRSP is a DCC user in the user role of "Import Supplier".

b) The ESA is not required to have an Interface M.

c) A CEM/ESAG is required to transmit power profile options created by the ESA from consumer preferences, external data and appliance information.

***NOTE** The system architecture for this configuration is shown in Figure D.3.*

Figure D.3 – Functional architecture for routine mode using Route 2: Tariff information via DCC WAN (e.g. ESA is internet enabled)



***NOTE** This is an example configuration, which shows an on-premises CEM. However, the CEM is a logical entity and may be sited outside the premises (i.e. cloud based). See Clause **4** for CEM configuration options.*

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 **5.5**.*

D.4.2 Route 3: Load control via APC

D.4.2.1 Process flow

The process flow is as follows.

a) The ESA is supplied with an APC, instantiated in an ESME or a SAPC.

   ***NOTE** APCs could be supplied as part of the CEM where the CEM is in the premises. In this situation each ESA would need a unique APC connection in the CEM.*

b) The ESA creates power profile options, for routine and response mode operation, from consumer preferences, external data and appliance information and sends them to the CEM/ESAG, via Interface B.

c) The CEM/ESAG translates the power profiles, each with unique numbers, into the Interface A specification and sends them to the ESA/APC, via Interface B.

d) The ESA/APC sends the information to the DSRSP as an event-based alert, via the Interface M. This alert is a container that can convey a fixed size of data, the format of this alert is defined in GBCS v4.0 [9]. Alerts can be concatenated where size requirements exceed a single alert. Power profile format is not defined in GBCS v4.0, but this could be introduced through a modification to GBCS using the Smart Energy Code modification process[10)].

e) 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.

f) During response mode, the DSRSP selects a power profile and sends the corresponding unique number to the ESA/APC.

g) The DSRSP passes the number to the DCC, which routes the number to the ESA/APC, via Interface M, using the communications hub and SMHAN.

h) The ESA/APC implements operation of the corresponding power profile.

i) The ESA/APC updates the power profiles accordingly and sends the updated profiles to the CEM/ESAG for translation and transmission to the DSRSP via the same route above (see also the following caveat).

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.

a) In order to support this configuration, the ESA is supplied with an APC interface and functionality. The APC functionality is instantiated in an ESME or SAPC. The provision of an APC interface means the ESA/APC has a Zigbee SE interface – the so-called "Interface M". Additionally, the ESA/APC is paired to the SMHAN and joined to the ESME/SAPC by a DCC user (e.g. DCC user roles: Import Supplier, "other user", etc.).

b) In order to support this configuration, the DSRSP is a DCC user in the user role of Import Supplier.

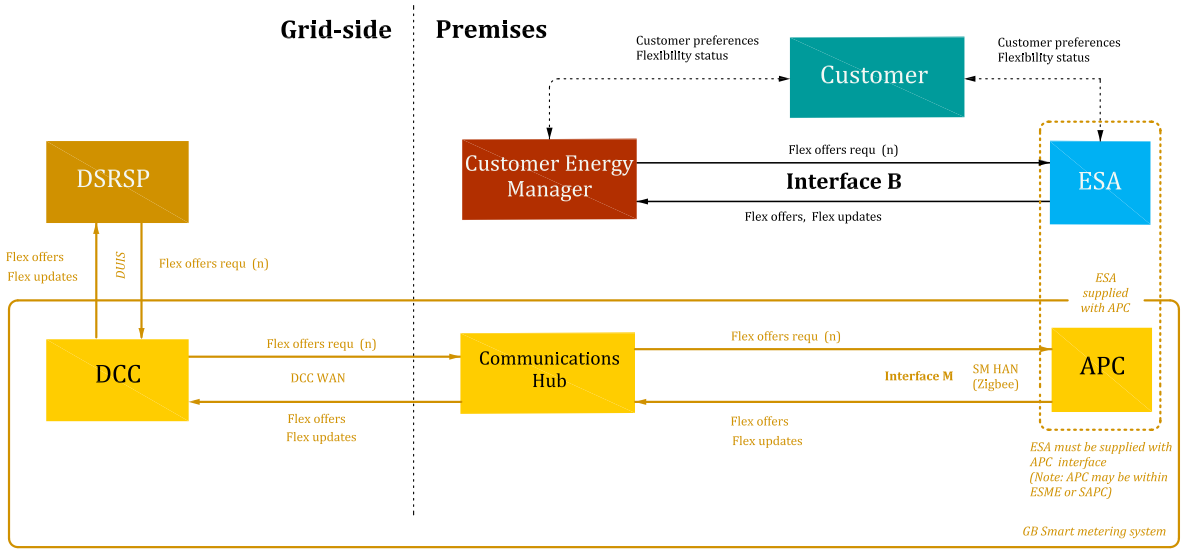
c) A CEM/ESAG is required in order to transmit power profile options created by the ESA from consumer preferences, external data and appliance information.

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 for this configuration is shown in Figure D.4.*

[10)] Available at https://smartenergycodecompany.co.uk/

Figure D.4 – Functional architecture for response mode using Route 3: Load control via APC (e.g. ESA supplied with APC)



***NOTE** This is an example configuration, which shows an on-premises CEM. However, the CEM is a logical entity and may be sited outside the premises (i.e. cloud based). See Clause **4** for CEM configuration options.*

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)
Relationship between the PAS functional architecture and representative CENELEC/IEC functional architecture

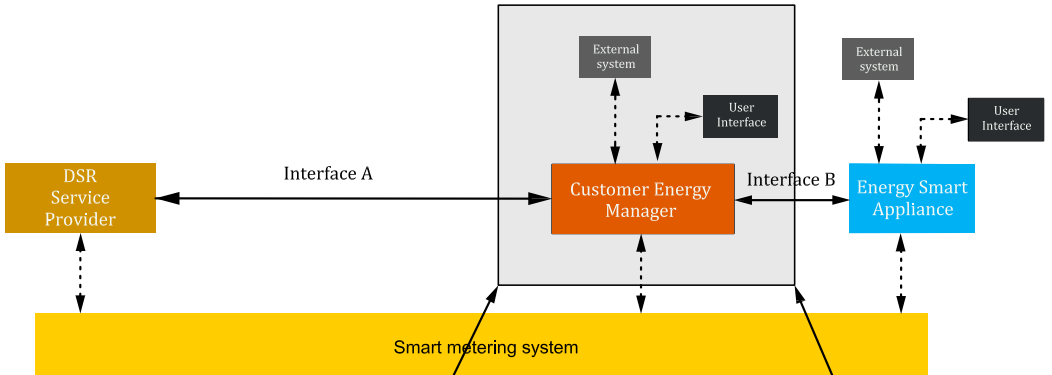
*COMMENTARY ON ANNEX **E***

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.

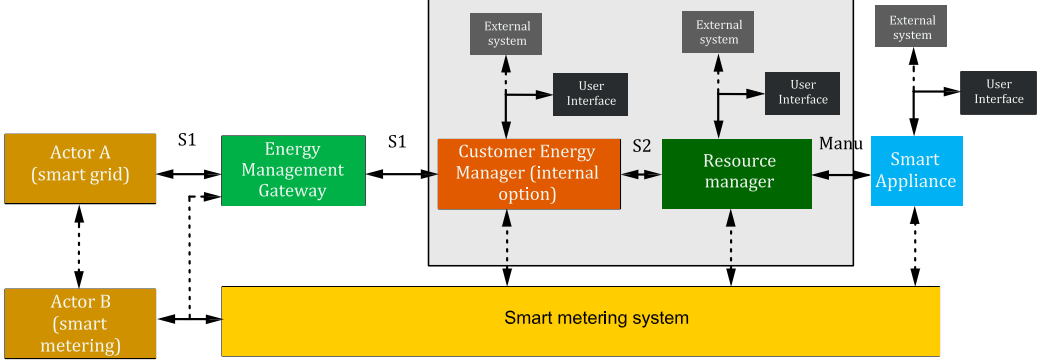
The two architectures and how they are mapped are shown in Figure E.1. The CENELEC/IEC architecture is configured assuming that the CEM is internal to the consumer premises. As this is a functional architecture, a configuration with the CEM external to the consumer premises (e.g. in the cloud) is also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

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

PAS 1878 architecture



CENELEC and IEC functional architecture representation



E.1 Description of CENELEC/IEC components and interfaces

NOTE Figure E.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 BS EN 50491-12-1:2018, BS EN 50631-1:2017, PD IEC/TR 62746-2:2015, and prEN50491-12-2.

E.1.1 Smart appliance

The smart appliance is a 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".

E.1.2 Resource Manager

The Resource Manager appears in BS EN 50491-12-1, prEN50491-12-2 and is implicitly included in the Customer Connectivity and Energy Manager (CCM) referred to in 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).

NOTE A Resource Manager may also be called an "ESA Gateway" (ESAG). The remaining functionality of the Resource Manager is yet to be fully defined and agreed.

E.1.3 Customer Energy Manager

The main task of the CEM is to relay messages between the grid-side Actor 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 consumer preferences, tariffs, DSR requests etc.

BS EN 50491-12-1 defines a CEM as: "internal automation function for optimizing the energy consumption, production and storage within the premises according to the preferences of the consumer using internal flexibilities and typically based on external information received through the Smart Grid Connection Point and possibly other data sources".

NOTE The remaining functionality of the CEM is yet to be fully defined and agreed.

E.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.

E.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 consumer premises (for example, to deliver DSR).

E.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 consumer premises.

E.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.

E.1.8 Interface B

This interface connects the Resource Manager with the Customer Energy Manager. This interface is described in EN 50491-12-1. For cases where 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.

NOTE The data model for this interface is being standardized in prEN 50491-12-2.

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.

E.1.9 Interface A

This interface 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.

NOTE OpenADR has been selected as a candidate in this PAS and has been specified accordingly, but other possible candidates include the IEC 61850 series, BS IEC 62746-10-1: 2018, EEBus or the development of a new standard.

E.2 Mapping of components and interfaces

*NOTE From the descriptions in E.1, the equivalent relationships depicted in Table E.1 may be derived. The mapping between the PAS 1878 and CENELEC/IEC components and interfaces are described in **E.2.1** to **E.2.9**.*

Table E.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

E.2.1 Smart Appliance

An ESA as defined in this PAS is very similar to a smart appliance as defined by CENELEC/IEC. Interface B represents a subset 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 IEC smart appliance is not.

E.2.2 Resource Manager

A separate Resource Manager is not a fundamental requirement within this PAS and the CEM is optionally able to take on this role.

This PAS does not restrict the use of a separate Resource Manager

E.2.3 Customer Energy Manager

The CEM in this PAS 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.

NOTE *This is equivalent to the CEM of EN 50491-12-1.*

E.2.4 Energy Management Gateway

The Energy Management Gateway is not explicitly described in this PAS. 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 this PAS. 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.

E.2.5 Actor A

Actor A is equivalent to the DSRSP.

E.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.

E.2.7 Interface "manufacturer"

This is equivalent to Interface B. Certain information model, messaging and cyber-security requirements are specified in this PAS, in order to support DSR operations. However, the details of the data model and underlying protocols are left to the manufacturer.

E.2.8 Interface S2

There is no requirement for an interoperable S2 interface described in this PAS. Although this is seen as further work, there is no restriction on the possible optional implementation of the S2 interface.

E.2.9 Interface S1

This is equivalent to Interface A. As Interface A is specified in this PAS, it is hoped that the definition will contribute to the international standardization of this interface.

Annex F (normative)
Interface A

*COMMENTARY ON **ANNEX F***

*The requirements for Interface A, including an information model, are provided in Clause **5** and Clause **6**. In order to provide a platform for an interoperable interface meeting these requirements, a communications protocol that supports the information model is required.*

This Annex describes the use of OpenADR within the context of PAS 1878, including the exchange of registration, initialization and flexibility offer information, and cybersecurity configuration.

The PAS 1878 information model is provided in a general form and has not been written from the point of view of any particular protocol implementation.

OpenADR 2.0b [16] was published as an IEC International Standard, IEC 62746-10-1:2018 in 2018 by IEC TC57 "Power systems management and associated information exchange".

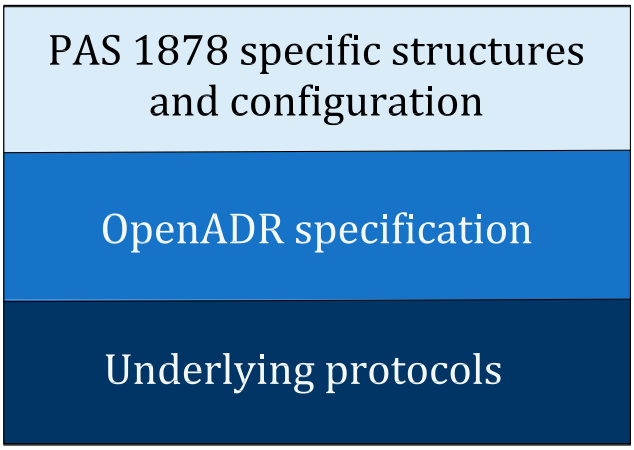
A related standard covering the compatibility of OpenADR with the Common Information Model (CIM), IEC 62746-10-3:2018 is also published by IEC TC57[11].

The OpenADR protocol is not modified in any material way by the Annex. Rather, the Annex provides a structure that is mapped on to the OpenADR protocol, as illustrated in Figure F.1. This structure includes the definition of which OpenADR services are to be used, the format (template) of the XML used within the payloads of those services and the use of the cybersecurity mechanisms inherent in the OpenADR specification.

F.1 Introduction

This PAS mandates that any implementation of Interface A shall support the use of OpenADR as described in this Annex and shall always revert to the use of OpenADR in order to guarantee interoperability. This PAS does not restrict the use of other protocols to implement Interface A and mandates that all such implementations shall meet the requirements of Clauses **5** and **6** of this PAS.

Figure F.1 – Alignment of Annex F to the OpenADR protocol definition



F.2 High level requirements

OpenADR encompasses many options which may be applied to produce a conformant implementation, but at a high level, certain options and non-typical configurations shall be specified by this Annex.

Interface A shall:

a) conform to OpenADR specification 2.0b or later;

b) perform mutual authentication over TLS;

c) implement the OpenADR High Security level (in order to support the use of digital signatures);

[11] IEC TC57 Dashboard. Accessible at: https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1273,25

d) require the optional OpenADR functionality that allows a VTN (Virtual Top Node, in this case the DSRSP) to be a report producer and the VEN (Virtual End Node, in this case the CEM) to be able to request reports from the VTN;

e) generate reports outside of the OpenADR reportBackDuration frequency;

f) require the CEM to support simpleHTTP and optionally XMPP; and

g) support the use of the *eiReportID* identifier (See Conformance Rule 339 of BS IEC 62746-10-1).

***NOTE** In addition, some interval durations used across Interface A are variable (rather than fixed). As a consequence, alignment between the VTN and VEN about the number of intervals per reportBackDuration period might be necessary.*

F.3 Registration and de-registration

The CEM/DSRSP registration and de-registration requirements included in **5.3.2**, **5.3.7**, **6.14.2.3** and **6.14.4** shall be implemented using the OpenADR 2.0b Registration Service as described in BS IEC 62746-10-1, 6.3.

In particular, these Registration Service messages shall be mapped to PAS 1878 requirements as shown in Table F.1.

In order for the CEM to be able to contact the DSRSP, it shall be provided with the DSRSP address out of band (by a means other than Interface A).

As described in **5.3.7**, if the CEM does not receive confirmation from the DSRSP that a de-registration request has been received following two re-tries, the CEM shall assume that the de-registration has been successful. Hence, if the CEM does not receive an *oadrCanceledRegistration* payload (message) following two *oadrCancelPartyRegistration* retries then it shall assume that the de-registration process has been successful and proceed accordingly.

All timing requirements specified in **5.3.7** shall be met.

F.4 Use of the OpenADR report service

Both CEM–DSRSP initialization and normal operation phases as defined in **5.4.3** and **5.4.4** shall be supported by use of the OpenADR Report Service as described in this clause.

Table F.1 – Relevant OpenADR Registration Service messages

Message payload	Source	Note
oadrQueryRegistration	CEM	Includes OpenADR protocol version number, communications capabilities etc. as described in BS IEC 62746-10-1, 6.3.2.
oadrCreatedPartyRegistration	DSRSP	Includes Registration ID, CEM ID etc. as described in BS IEC 62746-10-1, 6.3.2.
oadrCancelPartyRegistration	CEM or DSRSP	Cancel current registration.
oadrCreatePartyRegistration	CEM	Registration request to the DSRSP
oadrRequestReregistration	DSRSP	Request for CEM re-registration

The OpenADR Report Service payloads shall be used to convey information as shown in Table F.2.

Table F.2 – OpenADR Report Service payloads applied to "Initialization" and "Normal operation" phases

OpenADR Report Service payload	PAS 1878 information
oadrRegisterReport	(Part of "initialization" phase) From CEM: Reporting capability including flexibility offer types, power reporting types, (optionally) ESA Type and ESA Classification, CEM and ESA manufacturer name, serial number, EUI-64 and firmware version, failsafe mode notification, free text and security event log From CEM and DSRSP: DSR event cancellation capability
oadrCreateReport	(Part of "Initialization" phase) From DSRSP: Type of reports required from CEM (allows any optional reports to be selected, e.g. power reporting type) From CEM: Type of reports required from DSRSP
oadrUpdateReport	(Used during "Normal operation" phase) From CEM: All reports including flexibility offer reports, actual power profiles, instantaneous power consumption, DSR event cancellation, failsafe mode notification, security event log From DSRSP: All reports include flexibility offer request, DSR event cancellation

F.5 OpenADR report registration

F.5.1 General

The *oadrRegisterReport* payload, as described in BS IEC 62746-10-1, Clause 6.2 shall be used to convey the reporting properties of both the CEM and DSRSP.

F.5.2 CEM report registration payload

The CEM report registration payload is used to convey those elements of the PAS data model passed from the CEM to the DSRSP and shall include the following reports:

a) forecast power profile;
b) ESA current flexibility offer cancellation;
c) CEM initialization information;
d) ESA initialization information;
e) failsafe mode; and
f) security event log.

The CEM report registration payload shall also include at least one of the following reports:

1) actual power profile; and
2) periodic power report.

NOTE 1 *The CEM report registration payload can include the smart metering tariff.*

Additional information relating to specific flexibility offers, such as the order of the profile (e.g. LD, IO, MD, additional), profile class (i.e. consumption or production), Frequency Response Capability assigned to a specific forecast profile, the number of elements in the forecast profile and the source ESA, shall be included in the *eiReport* elements of specific reports in the CEM *oadrUpdateReport* payload.

NOTE 2 *Such information is not included in the* oadrRegisterReport *payload.*

The periodic power report (Instantaneous) power values shall be implemented as described in the OpenADR 2.0 Demand Response Program Implementation Guide [17], "A.4.2 Fast DR Scenario 2 – Typical Use Case, B profile", substituting the required reporting interval.

NOTE 3 *Electricity tariff values might be implemented using a structure based on the ELECTRICITY_PRICE signal in the OpenADR 2.0 DRP Implementation Guide [17], "A.1.3 CPP Scenario 3 – Complex Use Case". As the usage of tariff information is optional in this PAS and as the tariff structure will vary from country to country, a format agreed by the stakeholders within a particular country might be used.*

NOTE 4 *An example of the oadrRegisterReport payload listing for this structure is provided in Figure G.1.*

F.5.3 DSRSP report registration payload

The high level structure of the DSRSP payload shall be as depicted in Table F.2. A listing for this structure is provided in Figure G.2.

The DSRSP report registration payload is used to convey those elements of the PAS data model passed from the DSRSP to the CEM and shall include the following reports:

a) Flexibility offer request; and

b) DSRSP cancel current flexibility offer

F.5.4 OpenADR RegisterReport payload permitted values

*COMMENTARY ON **F.5.4***

This sub-clause defines the permitted range of values for various OpenADR parameters used in the CEM oadrRegistrationReport payload in order to support the mapping between the PAS 1878 information and the specific OpenADR implementation of Interface A.

F.5.4.1 Power forecast and actual power profiles

The nominal power *rID* values of the power forecast profiles (e.g. *x-FLEX_FORECAST-LD*, *x-FLEX_FORECAST-IO*, *x-FLEX_FORECAST-MD*) and the actual power profile (if supported) shall be represented as real values.

The characteristics of the real power value, defined by OpenADR *powerReal*, shall be set according to Table F.3.

Table F.3 – powerReal permitted values

powerReal values	Permitted value or range of values
ItemDescription	RealPower
ItemUnits	W or kW
siScaleCode	none or K
powerAttributes (hertz, voltage, ac)	Set by CEM according to local conditions

F.5.4.2 General timing

The *oadrSamplingrate* values are included in the metadata of many CEM reports and shall be set according to Table F.4.

Table F.4 – oadrSamplingRate permitted values

oadrSamplingRate values	Permitted value or range of values
oadrMinPeriod	1 s
oadrMaxPeriod	Depends upon CEM implementation but recommended 1000 hours
oadrOnChange	False

F.5.4.3 Report duration values

The *granularity duration*, *reportBackDuration* and *reportIntervalDuration* within the *oadrCreateReport* and *oadrRequestReport* payloads shall be as shown in Table F.5.

Table F.5 – oadrCreateReport and oadrRequestReport payload duration values

oadrCreateReport and oadrRequestReport Payload element	Permitted value or range of values
Granularity: duration	0 s
reportBackDuration: duration	24 h
reportInterval: duration: duration	0 s

F.5.5 Reporting templates

The structure of the Listings shall form the template for the CEM and DSRSP *oadrRegisterReport*, *oadrCreateReport* and *oadrUpdateReport* payloads, respectively.

In these templates, any parameter pre-pended with "*imp_*" shall be for assignment either by the CEM or by the OpenADR implementation according to any limits described in this Annex.

***NOTE** The listings can be found at Figure G.1, Figure G.2 and Figure G.3.*

F.6 OpenADR report selection

F.6.1 Selection of DSRSP reports

The CEM *oadrCreateReport* payload shall request all reports provided in the DSRSP *oadrRegisterReport* payload.

F.6.2 Selection of CEM reports

The OpenADR reports produced by the CEM and selected by the DSRSP (e.g. flexibility offers, instantaneous power value reporting) shall be denoted in an *oadrCreateReport* payload, according to BS IEC 62746-10-1, 6.2.

The DSRSP *oadrCreateReport* payload shall request all reports provided in the CEM *oadrRegisterReport* payload with the exception of the "Actual power profile", "Period power report" and "Smart metering tariff" reports.

At least one of the "Actual power profile" and "instantaneous power reporting" reports shall be selected.

***NOTE** The DSRSP may request the "Smart metering tariff report" if required.*

F.6.3 OpenADR *CreateReport* payload permitted values

*COMMENTARY ON **F.6.3***

This sub-clause defines the permitted range of values for various OpenADR parameters used in the CEM oadrCreateReport *payload in order to support the mapping between the PAS1878 information and the specific OpenADR implementation of Interface A.*

The PAS 1878 information model is provided in a general form and has not been written from the point of view of any particular protocol implementation.

F.6.3.1 Report duration values

The granularity duration, *reportBackDuration* and *reportIntervalDuration* within the *oadrCreateReport* payload shall be as shown in Table F.6.

Table F.6 – oadrCreateReport payload duration values

oadrCreateReport **Payload element**	**Permitted value or range of values**
Granularity: duration	0 s
reportBackDuration: duration	24 h
reportInterval: duration: duration	0 s

F.7 OpenADR update reports

F.7.1 General

The *oadrUpdateReport* payload, as described in BS IEC 62746-10-1, 6.2 shall be used to convey DSR information described in **5.4.4** between the DSRSP and CEM in the Normal Operation phase.

***NOTE** An example of the CEM* oadrUpdateReport *payload is shown in Figure G.3.*

Most values within the *oadrReportPayload* sections shall be provided by the CEM and DSRSP accordingly. However, the *oadrDataQuality* element of the *oadrUpdatePayload* shall be set to "*Quality Good – Non Specific*".

F.7.2 CEM to DSRSP

F.7.2.1 Initialization information

Information passed from the CEM to the DSRSP in the initialization phase (see **5.4.3**) shall be included in the *x-INFO* report of the *oadrUpdateRepor*t payload.

The type of information contained in this report shall be denoted using the *INFO_TYPE rID* value and the specific information shall be included in the *eiReportID* field.

The permitted *rID* values shall be as indicated in Table F.7.

Table F.7 – Allowed info_type rID value for CEM and ESA initialization information

Info_type rID value	**Meaning**
1.0	CEM initialization information
2.0	ESA initialization information

The specific information shall be included in the *eiReportID* field in the following manner:

Parameter:value;parameter:value;parameter:value…

The parameters and allowed values for *rID*=1.0 shall be as depicted in Table F.8.

Table F.8 – Information contained in x-INFO report, rID=1.0, eiReportID field

Parameter	Description	Permitted values	Mandatory/Optional
CEM_Aver	Version of Interface A supported by CEMs	String	M
CEM_Manu	CEM manufacturer or service provider name	String	M
CEM_SN	CEM serial number	String	M
CEM_EUI	CEM EUI-64	String	M
CEM_FW	CEM firmware version	String	M
CEM_SW	CEM software version	String	O
FreeTxt	Free text	String	O

The parameters and allowed values for *rID*=2.0 shall be as depicted in Table F.9.

Table F.9 – Information contained in x-INFO report, rID=2.0, eiReportID field

Parameter	Description	Permitted values	Mandatory/Optional
ESA_ID	Specific ESA identifier, supplied either by the ESA or the CEM.	String	O
ESA_Type	ESA Type, as defined in Annex C	As depicted in **Annex C**	O
ESA_Class	ESA Type, as defined in Annex C	As depicted in **Annex C** (min/max)	O
ESA_Manu	ESA manufacturer or service provider name	String	M
ESA_SN	ESA serial number	String	M
ESA_EUI	ESA EUI-64	String	M
ESA_FW	ESA firmware version	String	M
ESA_SW	ESA software version	String	O
FreeTxt	Free text	String	O

F.7.2.2 Flexibility offers

Flexibility offers shall consist of a set of forecast power profiles, each associated with a frequency response capability, and an indication of whether the forecast profile relates to power consumption or power production.

NOTE 1 *Optional information might also be included.*

Each forecast profile (e.g. LD, IO, MD, LD_P, MD_P and optional additional profiles) shall be included in separate *oadrReport* payloads within the *x-FLEX_FORECAST* report of the *oadrUpdateReport* payload.

Additional, associated, information shall be included in the *eiReportID* fields in the following manner:

Parameter:value;parameter:value;parameter:value…

The parameters and allowed values shall be as depicted in Table F.10.

Table F.10 – Flexibility offer – information contained in eiReportID

Parameter	Description	Permitted values	Mandatory/Optional
Order	Whether the profile is one of the defined set (LD, IO, MD, LD_P, MD_P) or optional additional profile index	LD, IO, MD, LD_P, MD_P, 1-995	M
FRC	Frequency Response Capability applied to this profile	As depicted in **5.4.5.1.1** Table 8	M
Intervals	Number of interval elements in the profile	0-999	M
ESA_ID	Specific ESA identifier, supplied either by the ESA or the CEM.	Free text (recommended short)	O

As described in **5.5.4.1**, at least ESA LD and MD frequency response capability values, and at least ESA LD, IO and MD power forecast profiles shall be included. If the ESA supports power production, then the "production" forecast power profiles, LD_P and MD_P, and their associated frequency response capabilities, shall also be included.

NOTE 2 *Forecast profile power values can be positive (consumption) and/or negative (production).*

The total number of forecast power profiles shall not exceed 1000.

As described in **5.5.4** the forecast power profiles shall have the capacity to contain interruptible and non-interruptible intervals, standardized interruption mechanism is for consideration in future versions of this PAS.

Whenever a new set of frequency response capability and forecast power profile information is issued in an *oadrUpdateReport* all such previous information shall be deemed obsolete.

F.7.2.3 Actual power profile

If the DSRSP has included the actual power report in its *CreateReport* payload, then the CEM shall provide an actual power profile report to the DSRSP following completion of a DSR event, as described in **5.4.5.1.3**.

NOTE *The CEM may include an optional "ESA_ID" parameter (see Table 10) in the* eiReportID *field of the Actual profile payload.*

F.7.2.4 Cancellation of current flexibility offer

This signalling shall be provided by the CEM in the *x-FLEX_ESA_CANCEL* report. The mapping of the *rID* values of this payload to the Cancel flexibility offer status (see **5.4.5.1.6**) shall be as shown in Table F.11.

Table F.11 – Mapping of cancellation rID (CEM cancellation)

ESA_CANCEL_CURRENT rID value	Cancel flexibility offer status
1.0	Cancel current flexibility offer

The CEM may include an optional "ESA_ID" parameter (see Table F.10) in the *eiReportID* field of the Actual profile payload.

F.7.2.5 Entering Failsafe mode

The indication from the CEM to the DSRP that either the CEM or an ESA is entering Failsafe Mode shall be included in the *x-INFO* report of the *oadrUpdateReport* payload.

The type of information contained in this report shall be denoted using the *info_type* rID value and the specific information shall be included in the *eiReportID* field.

The permitted rID value shall be as indicated in Table F.12.

Table F.12 – Allowed info_type rID value for CEM and/or ESA entering FailSafe Mode information

Head	Meaning
3.0	CEM and/or ESA Failsafe Mode notification

The specific information shall be included in the *eiReportID* field in the following manner:

Parameter:value;parameter:value;parameter:value…

The parameters and allowed values for rID=3.0 shall be as depicted in Table F.13. Multiple ESA notifications shall be implemented using multiple (ESA_FSM, ESA_ID) values.

Table F.13 – Information contained in x-INFO report, rID=3.0, eiReportID field

Parameter	Description	Permitted values	Mandatory/Optional
CEM_FSM	CEM entering Failsafe Mode	TRUE, FALSE	M
ESA_FSM	ESA entering Failsafe Mode	TRUE, FALSE	M
ESA_ID	Specific ESA identifier, supplied either by the ESA or the CEM (associated with immediately previous ESA_FSM parameter)	String	M (if ESA_FSM present)
FreeTxt	Free text	String	O

F.7.2.6 Security event log transfer

The security event log of either the CEM or an ESA shall be included in the *x-INFO* report of the *oadrUpdateReport* payload.

The type of information contained in this report shall be denoted using the *info_type* rID value and the specific information shall be included in the *eiReportID* field.

The permitted rID value shall be as indicated in Table F.14.

Table F.14 – Allowed info_type rID value for CEM and/or ESA security event log information

Info_type rID value	Meaning
4.0	CEM and/or ESA secure event log

The specific information shall be included in the *eiReportID* field in the following manner:

Parameter:value;parameter:value;parameter:value…

The parameters and allowed values for rID=4.0 shall be as depicted in Table F.15. Multiple ESA notifications shall be implemented using multiple (ESA_FSM, ESA_ID) values.

Table F.15 – Information contained in x-INFO report, rID=4.0, eiReportID field

Parameter	Description	Permitted values	Mandatory/Optional
CEM_SEL	CEM security event log	See	M
ESA_SEL	ESA security event log	See	M
ESA_ID	Specific ESA identifier, supplied either by the ESA or the CEM (associated with immediately previous ESA_FSM parameter)	String	M (if ESA_SEL present)
FreeTxt	Free text	String	O

The security event log, as described in **6.11**, shall consist of any or all of the timestamped indicators shown in Table F.16 and shall be formatted as:

Time_stamp: Parameter: Value; Time_stamp: Parameter: Value;…

The FreeTxt parameter may be used to include additional information, as required.

Table F.16 – Allowed security event log notification parameters

Parameter	Description	Permitted values	Mandatory/Optional
Auth_attempt	Request to attempt authorization with CEM or ESA successful/not successful	TRUE/FALSE	M
FW_inst_attempt	Firmware on CEM or ESA successfully/ unsuccessfully installed	TRUE/FALSE	M
SW_inst_attempt	Software on CEM or ESA successfully/ unsuccessfully installed	TRUE/FALSE	M
Comms_port	Authorized/ unauthorized attempt to access communications port	TRUE/FALSE	M
Event_type	See Table F.17	See Table F.17	M
Unauth_msg	Reception of an unauthorized message	TRUE	M
FreeTxt	Free text	String	O

Table F.17 – Event_type parameters and permitted values

Parameter	Description	Permitted values
Msgs_Tx	Number messages sent (over a certain threshold, within a certain time period)	Positive floating point number (rounded to integer equivalent)
Msgs_Rx	Number messages received (over a certain threshold, within a certain time period)	Positive floating point number (rounded to integer equivalent)
Msgs_actioned	Number messages acted upon (over a certain threshold, within a certain time period)	Positive floating point number (rounded to integer equivalent)

F.7.3 DSRSP to CEM flexibility offer request

The CEM shall receive the DSRSP flexibility offer request using the rID *Flexibility_Offer_Select* of the *x-FLEX-OFFER-REQUEST* report within the DSRSP oadrUpdateReport payload.

The *Flexibility_Offer_Select* value shall correspond to the position of the chosen forecast power profile within the set previously provided by the CEM and shall be set to a value between 0.0 (first forecast power profile) and 1000.0 in 1.0 increments (the IO forecast power profile shall never be selected).

The DSRSP frequency response maximum and minimum frequency limits shall be conveyed in the rID *Flexibility_Offer_Frequ_Response_Max* and rID *Flexibility_Offer_Frequ_Response_Min*, as described in **5.4.5.2.2**.

F.7.4 Cancellation of current flexibility offer

This signalling shall be provided by the DSRSP in the *x-FLEX_DSRSP_CANCEL* report. The mapping of the rID value of this payload to the Cancel flexibility offer status (see **5.4.5.2.3**) shall be as shown in Table F.18.

Table F.18 – Mapping of cancellation rID (DSRSP cancellation)

ESA_CANCEL_CURRENT and *DSRSP_CANCEL_CURRENT* rID value	Cancel flexibility offer status
1.0	Cancel current flexibility offer

F.8 Cybersecurity

*COMMENTARY ON **F.8***

This Clause explains the relationship between OpenADR cybersecurity mechanisms within the context of the relevant PAS 1878 requirements.

F.8.1 General

Interface A shall conform to all OpenADR security requirements and specifications.

F.8.2 Secure protocols and cipher suites

In line with Clause 5 of this PAS, Interface A shall support TLS v1.3 and cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

In line with the optionality described in in BS IEC 62746-10-1, 8.5 and Conformance Rule 67, the OpenADR security sub-system shall make use of TLS 1.2 or later (allowing mutual authentication) and currently makes use of the following cipher suites:

- ECC – TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- RSA – TLS_RSA_WITH_AES_128_CBC_SHA256

However, the OpenADR cipher suites are specified in line with NIST SP 800-131 and so any implementation of Interface A shall comply with any OpenADR security updates made in line with NIST SP 800-131.

F.8.3 Authentication

*COMMENTARY ON **F.8.3***

OpenADR specifies the use of X.509 certificates as part of the TLS process. In addition, the use of Certificate Fingerprints is included in order to provide an additional level of authentication.

Interface A shall make use of OpenADR Certification Fingerprints in addition to TLS/X.509 authentication.

F.8.4 Signatures

Interface A shall use the OpenADR "high security" level which enables the use of XML signatures to sign either the whole or portions of the XML document as described in BS IEC 62746-10-1, 8.7.

Annex G (informative) XML code examples

The figures in this Annex provide example Listings of PAS 1878 OpenADR XML code for registration and update report payloads in accordance with the previous descriptions.

NOTE *In Figures G1 and G2 any parameter pre-pended with "imp_" is for assignment either by the CEM or by the OpenADR implementation according to any limits described in Annex F.*

Figure G.1 – Listing #1: CEM oadrRegisterReport payload

```
<oadr:oadrPayload>
<oadr:oadrSignedObject>
  <oadr:oadrRegisterReport ei:schemaVersion="2.0b">
    <pyld:requestID>imp_requestID_4322</pyld:requestID>


    <!-- **** FORECAST PROFILE **** -->

    <oadr:oadrReport>
      <xcal:duration>
        <xcal:duration>PT1000H</xcal:duration>
      </xcal:duration>
      <oadr:oadrReportDescription>
          <ei:rID>NominalPower_consumption</ei:rID>
          <ei:reportDataSource>
          <ei:resourceID>imp_CEM_ID_CompanyName_54342</ei:resourceID>
          </ei:reportDataSource>
        <ei:reportType>x-NotApplicable</ei:reportType>
        <oadr:powerReal>
          <oadr:itemDescription>RealPower</oadr:itemDescription>
          <oadr:itemUnits>imp_W</oadr:itemUnits>
          <scale:siScaleCode>imp_none</scale:siScaleCode>
          <oadr:powerAttributes>
            <oadr:hertz>imp_50</oadr:hertz>
            <oadr:voltage>imp_240</oadr:voltage>
            <oadr:ac>imp_true</oadr:ac>
          </oadr:powerAttributes>
        </oadr:powerReal>
        <ei:readingType>x-NotApplicable</ei:readingType>
        <emix:marketContext>http://MarketContext1</emix:marketContext>
        <oadr:oadrSamplingRate>
          <oadr:oadrMinPeriod>PT1S</oadr:oadrMinPeriod>
          <oadr:oadrMaxPeriod>PT1000H</oadr:oadrMaxPeriod>
          <oadr:oadrOnChange>false</oadr:oadrOnChange>
        </oadr:oadrSamplingRate>
      </oadr:oadrReportDescription>
      <ei:reportRequestID>0</ei:reportRequestID>
      <ei:reportSpecifierID>reportSpecifierID_FPP</ei:reportSpecifierID>
      <ei:reportName>x-METADATAx-FLEX_FORECAST</ei:reportName>
      <ei:createdDateTime>imp_2020-10-11T23:54:22Z</ei:createdDateTime>
     </oadr:oadrReport>


<!-- **** ACTUAL POWER PROFILE **** -->
     <oadr:oadrReport>
      <xcal:duration>
        <xcal:duration>PT1000H</xcal:duration>
      </xcal:duration>
      <oadr:oadrReportDescription>
          <ei:rID>NominalPower_APP</ei:rID>
          <ei:reportDataSource>
          <ei:resourceID>imp_CEM_ID_CompanyName_54342</ei:resourceID>
          </ei:reportDataSource>
        <ei:reportType>x-NotApplicable</ei:reportType>
        <oadr:powerReal>
          <oadr:itemDescription>RealPower</oadr:itemDescription>
          <oadr:itemUnits>imp_W</oadr:itemUnits>
          <scale:siScaleCode>imp_none</scale:siScaleCode>
          <oadr:powerAttributes>
            <oadr:hertz>imp_50</oadr:hertz>
            <oadr:voltage>imp_240</oadr:voltage>
            <oadr:ac>imp_true</oadr:ac>
          </oadr:powerAttributes>
        </oadr:powerReal>
        <ei:readingType>x-NotApplicable</ei:readingType>
```

Figure G.1 – Listing #1: CEM oadrRegisterReport payload *(continued)*

```
67.           <emix:marketContext>http://MarketContext1</emix:marketContext>
68.           <oadr:oadrSamplingRate>
69.             <oadr:oadrMinPeriod>PT1S</oadr:oadrMinPeriod>
70.             <oadr:oadrMaxPeriod>PT1000H</oadr:oadrMaxPeriod>
71.             <oadr:oadrOnChange>false</oadr:oadrOnChange>
72.           </oadr:oadrSamplingRate>
73.         </oadr:oadrReportDescription>
74.         <ei:reportRequestID>0</ei:reportRequestID>
75.         <ei:reportSpecifierID>reportSpecifierID_APP</ei:reportSpecifierID>
76.         <ei:reportName>x-METADATAx-FLEX_Actual_PWR_Profile</ei:reportName>
77.         <ei:createdDateTime>imp_2020-10-11T23:54:22Z</ei:createdDateTime>
78.       </oadr:oadrReport>
79.
80.
81.
82. <!-- **** ESA current flex offer cancellation **** -->
83.       <oadr:oadrReport>
84.         <xcal:duration>
85.           <xcal:duration>PT1000H</xcal:duration>
86.         </xcal:duration>
87.         <oadr:oadrReportDescription>
88.           <ei:rID>ESA_CANCEL_CURRENT</ei:rID>
89.           <ei:reportDataSource>
90.             <ei:resourceID>imp_CEM_ID_CompanyName_54342</ei:resourceID>
91.           </ei:reportDataSource>
92.           <ei:reportType>level</ei:reportType>
93.           <ei:readingType>x-NotApplicable</ei:readingType>
94.           <emix:marketContext>http://MarketContext1</emix:marketContext>
95.           <oadr:oadrSamplingRate>
96.             <oadr:oadrMinPeriod>PT1M</oadr:oadrMinPeriod>
97.             <oadr:oadrMaxPeriod>PT1000H</oadr:oadrMaxPeriod>
98.             <oadr:oadrOnChange>false</oadr:oadrOnChange>
99.           </oadr:oadrSamplingRate>
100.              </oadr:oadrReportDescription>
101.              <ei:reportRequestID>0</ei:reportRequestID>
102.              <ei:reportSpecifierID>reportSpecifierID_ESA_CANCEL_CURRENT</ei:rep
    ortSpecifierID>
103.              <ei:reportName>x-METADATAx-FLEX_ESA_CANCEL</ei:reportName>
104.              <ei:createdDateTime>2020-10-11T23:54:22Z</ei:createdDateTime>
105.            </oadr:oadrReport>
106.
107.      <!-- **** CEM and ESA Information **** -->
108.            <oadr:oadrReport>
109.              <xcal:duration>
110.                <xcal:duration>PT1000H</xcal:duration>
111.              </xcal:duration>
112.              <oadr:oadrReportDescription>
113.                <ei:rID>INFO_TYPE</ei:rID>
114.                <ei:reportDataSource>
115.                  <ei:resourceID>imp_CEM_ID_CompanyName_54342</ei:resourceID>
116.                </ei:reportDataSource>
117.                <ei:reportType>level</ei:reportType>
118.                <ei:readingType>x-NotApplicable</ei:readingType>
119.                <emix:marketContext>http://MarketContext1</emix:marketContext>
120.                <oadr:oadrSamplingRate>
121.                  <oadr:oadrMinPeriod>PT1M</oadr:oadrMinPeriod>
122.                  <oadr:oadrMaxPeriod>PT1000H</oadr:oadrMaxPeriod>
123.                  <oadr:oadrOnChange>false</oadr:oadrOnChange>
124.                </oadr:oadrSamplingRate>
125.              </oadr:oadrReportDescription>
126.              <ei:reportRequestID>0</ei:reportRequestID>
127.              <ei:reportSpecifierID>reportSpecifierID_CEM_ESA_INFO</ei:reportSpe
    cifierID>
128.              <ei:reportName>x-METADATAx-CEM_ESA_INFO</ei:reportName>
129.              <ei:createdDateTime>2020-10-11T23:54:22Z</ei:createdDateTime>
130.            </oadr:oadrReport>
```

Figure G.1 – Listing #1: CEM oadrRegisterReport payload *(continued)*

```
131.
132.                    <ei:venID>imp_venID_54342</ei:venID>
133.                </oadr:oadrRegisterReport>
134.            </oadr:oadrSignedObject>
135.        </oadr:oadrPayload>
```

Figure G.2 – Listing #2: DSRSP oadrRegisterReport payload

```
<oadr:oadrPayload>
  <oadr:oadrSignedObject>
    <oadr:oadrRegisterReport ei:schemaVersion="2.0b">
      <pyld:requestID>imp_requestID_4322</pyld:requestID>

      <!-- **** Flexibility Offer Request **** -->
      <oadr:oadrReport>
        <xcal:duration>
          <xcal:duration>PT1000H</xcal:duration>
        </xcal:duration>

        <!-- **** Select flex offer (which profile) **** -->
        <oadr:oadrReportDescription>
            <ei:rID>Flexibility_Offer_Select</ei:rID>
            <ei:reportDataSource>
                <ei:resourceID>imp_DSRSP_ID_CompanyName_54342</ei:resourceID>
            </ei:reportDataSource>
            <ei:reportType>level</ei:reportType>
            <ei:readingType>x-NotApplicable</ei:readingType>
            <emix:marketContext>http://MarketContext1</emix:marketContext>
            <oadr:oadrSamplingRate>
                <oadr:oadrMinPeriod>PT1S</oadr:oadrMinPeriod>
                <oadr:oadrMaxPeriod>PT1000H</oadr:oadrMaxPeriod>
                <oadr:oadrOnChange>false</oadr:oadrOnChange>
            </oadr:oadrSamplingRate>
        </oadr:oadrReportDescription>
        <ei:reportRequestID>0</ei:reportRequestID>
        <ei:reportSpecifierID>DSRSP_reportSpecifierID_FOR</ei:reportSpecifierID>

        <ei:reportName>x-METADATAx-FLEX_OFFER_REQUEST</ei:reportName>
        <ei:createdDateTime>imp_2020-10-11T23:54:22Z</ei:createdDateTime>
       </oadr:oadrReport>

        <!-- **** Select flex offer (frequency response capability) **** -->
        <oadr:oadrReportDescription>
            <ei:rID>Flexibility_Offer_Frequ_Response_Max</ei:rID>

            <ei:reportDataSource>
                <ei:resourceID>imp_DSRSP_ID_CompanyName_54342</ei:resourceID>
            </ei:reportDataSource>
            <ei:reportType>level</ei:reportType>
            <ei:readingType>x-NotApplicable</ei:readingType>
            <emix:marketContext>http://MarketContext1</emix:marketContext>
            <oadr:oadrSamplingRate>
                <oadr:oadrMinPeriod>PT1S</oadr:oadrMinPeriod>
                <oadr:oadrMaxPeriod>PT1000H</oadr:oadrMaxPeriod>
                <oadr:oadrOnChange>false</oadr:oadrOnChange>
            </oadr:oadrSamplingRate>
            <ei:rID>Flexibility_Offer_Frequ_Response_Min</ei:rID>

            <ei:reportDataSource>
                <ei:resourceID>imp_DSRSP_ID_CompanyName_54342</ei:resourceID>
            </ei:reportDataSource>
            <ei:reportType>level</ei:reportType>
            <ei:readingType>x-NotApplicable</ei:readingType>
            <emix:marketContext>http://MarketContext1</emix:marketContext>
            <oadr:oadrSamplingRate>
                <oadr:oadrMinPeriod>PT1S</oadr:oadrMinPeriod>
                <oadr:oadrMaxPeriod>PT1000H</oadr:oadrMaxPeriod>
                <oadr:oadrOnChange>false</oadr:oadrOnChange>
            </oadr:oadrSamplingRate>
        </oadr:oadrReportDescription>

        <ei:reportRequestID>0</ei:reportRequestID>
        <ei:reportSpecifierID>DSRSP_reportSpecifierID_FCR</ei:reportSpecifierID>
```

Figure G.2 – Listing #2: DSRSP oadrRegisterReport payload *(continued)*

```
        <ei:reportName>x-METADATAx-FLEX_OFFER_REQUEST</ei:reportName>
        <ei:createdDateTime>imp_2020-10-11T23:54:22Z</ei:createdDateTime>
      </oadr:oadrReport>

      <!-- **** ESA current flex offer cancellation **** -->
      <oadr:oadrReport>
      <xcal:duration>
        <xcal:duration>PT1000H</xcal:duration>
      </xcal:duration>
      <oadr:oadrReportDescription>
        <ei:rID>DSRSP_CANCEL_CURRENT</ei:rID>
        <ei:reportDataSource>
          <ei:resourceID>imp_CEM_ID_CompanyName_54342</ei:resourceID>
        </ei:reportDataSource>
        <ei:reportType>level</ei:reportType>
        <ei:readingType>x-NotApplicable</ei:readingType>
        <emix:marketContext>http://MarketContext1</emix:marketContext>
        <oadr:oadrSamplingRate>
          <oadr:oadrMinPeriod>PT1M</oadr:oadrMinPeriod>
          <oadr:oadrMaxPeriod>PT1000H</oadr:oadrMaxPeriod>
          <oadr:oadrOnChange>false</oadr:oadrOnChange>
        </oadr:oadrSamplingRate>
      </oadr:oadrReportDescription>
      <ei:reportRequestID>0</ei:reportRequestID>
      <ei:reportSpecifierID>reportSpecifierID_DSRSP_CANCEL_CURRENT</ei:reportSp
ecifierID>
      <ei:reportName>x-METADATAx-FLEX_ESA_CANCEL</ei:reportName>
      <ei:createdDateTime>2020-10-11T23:54:22Z</ei:createdDateTime>
      </oadr:oadrReport>

      <ei:venID>imp_venID_54342</ei:venID>
    </oadr:oadrRegisterReport>
  </oadr:oadrSignedObject>
</oadr:oadrPayload>
```

Figure G.3 – Listing #3: (see Figs G.1 and G.2) Example CEM oadrUpdateReport payload

```
<oadr:oadrPayload>
  <oadr:oadrSignedObject>
    <oadr:oadrUpdateReport ei:schemaVersion="2.0b">
      <pyld:requestID>requestID_4324</pyld:requestID>

      <!-- **** CEM INITIALISATION INFORMATION  **** -->
      <oadr:oadrReport>

      <!-- **** Start time  **** -->
        <xcal:dtstart>
          <xcal:date-time>2020-10-11T23:59:27Z</xcal:date-time>
        </xcal:dtstart>

        <strm:intervals>
          <ei:interval>
            <xcal:duration>
               <xcal:duration>PT10S</xcal:duration>
            </xcal:duration>
            <oadr:oadrReportPayload>
             <ei:rID>INFO_TYPE</ei:rID>
             <ei:payloadFloat>
                <ei:value>1.0</ei:value>
             </ei:payloadFloat>
             <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadrDataQua
lity>
            </oadr:oadrReportPayload>
          </ei:interval>

        </strm:intervals>
        <ei:eiReportID>CEM_Aver:1.0;CEM_Manu:CEM_ACME;CEM_SN:9876AB5432;CEM_EUI:9
073.1AFF.FE78.9B17;CEM_FW:1.7.3;CEM_SW:7.8.2</ei:eiReportID>
        <ei:reportRequestID>reportRequest_5678</ei:reportRequestID>
        <ei:reportSpecifierID>reportSpecifierID_CEM_ESA_INFO_5678</ei:reportSpeci
fierID>
        <ei:reportName>x-CEM_ESA_INFO</ei:reportName>
        <ei:createdDateTime>2020-10-11T23:59:27Z</ei:createdDateTime>
    </oadr:oadrReport>

      <!-- **** ESA INITIALISATION INFORMATION  **** -->
      <oadr:oadrReport>

      <!-- **** Start time  **** -->
        <xcal:dtstart>
          <xcal:date-time>2020-10-11T23:59:27Z</xcal:date-time>
        </xcal:dtstart>

        <strm:intervals>
          <ei:interval>
            <xcal:duration>
               <xcal:duration>PT10S</xcal:duration>
            </xcal:duration>
            <oadr:oadrReportPayload>
             <ei:rID>INFO_TYPE</ei:rID>
             <ei:payloadFloat>
                <ei:value>2.0</ei:value>
             </ei:payloadFloat>
             <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadrDataQua
lity>
            </oadr:oadrReportPayload>
          </ei:interval>

        </strm:intervals>
        <ei:eiReportID>ESA_ID:ESA#1;ESA_Type:5;ESA_Class:0/2;ESA_Manu:ESA_ACME;ES
A_SN:UY-B7-
JT41_UK;ESA_EUI:3063.1AFF.FE98.931A;ESA_FW:6.4;ESA_SW:2.4.6 </ei:eiReportID>
        <ei:reportRequestID>reportRequest_5678</ei:reportRequestID>
```

Figure G.3 – Listing #3: (see Figs G.1 and G.2) Example CEM oadrUpdateReport payload *(continued)*

```
61.         <ei:reportSpecifierID>reportSpecifierID_CEM_ESA_INFO_5678</ei:reportSpeci
    fierID>
62.         <ei:reportName>x-CEM_ESA_INFO</ei:reportName>
63.         <ei:createdDateTime>2020-10-11T23:59:27Z</ei:createdDateTime>
64.     </oadr:oadrReport>
65.
66.       <!-
    - **** FORECAST PROFILE, LD,  FREQU RESP CAP=1, 4X INTERVALS, FROM ESA#1  **** --
    >
67.       <oadr:oadrReport>
68.
69.       <!-- **** Start time  **** -->
70.         <xcal:dtstart>
71.           <xcal:date-time>2020-10-11T23:59:27Z</xcal:date-time>
72.         </xcal:dtstart>
73.
74.         <strm:intervals>
75.           <ei:interval>
76.             <xcal:duration>
77.                <xcal:duration>PT10S</xcal:duration>
78.             </xcal:duration>
79.             <oadr:oadrReportPayload>
80.              <ei:rID>x-Nominal_Power</ei:rID>
81.              <ei:payloadFloat>
82.                 <ei:value>3.0</ei:value>
83.               </ei:payloadFloat>
84.               <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadrDataQua
    lity>
85.             </oadr:oadrReportPayload>
86.           </ei:interval>
87.
88.           <ei:interval>
89.             <xcal:duration>
90.                <xcal:duration>PT3S</xcal:duration>
91.             </xcal:duration>
92.             <oadr:oadrReportPayload>
93.              <ei:rID>x-Nominal_Power</ei:rID>
94.              <ei:payloadFloat>
95.                 <ei:value>2000.0</ei:value>
96.               </ei:payloadFloat>
97.               <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadrDataQua
    lity>
98.             </oadr:oadrReportPayload>
99.           </ei:interval>
100.
101.                <ei:interval>
102.                  <xcal:duration>
103.                     <xcal:duration>PT60M</xcal:duration>
104.                  </xcal:duration>
105.                  <oadr:oadrReportPayload>
106.                   <ei:rID>x-Nominal_Power</ei:rID>
107.                   <ei:payloadFloat>
108.                      <ei:value>10000.0</ei:value>
109.                    </ei:payloadFloat>
110.                    <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
    DataQuality>
111.                  </oadr:oadrReportPayload>
112.                </ei:interval>
113.
114.                <ei:interval>
115.                  <xcal:duration>
116.                    <xcal:duration>PT10M</xcal:duration>
117.                  </xcal:duration>
118.                  <oadr:oadrReportPayload>
119.                  <ei:rID>x-Nominal_Power</ei:rID>
120.                  <ei:payloadFloat>
```

Figure G.3 – Listing #3: (see Figs G.1 and G.2) Example CEM oadrUpdateReport payload *(continued)*

```
                        <ei:value>200.0</ei:value>
                    </ei:payloadFloat>
                    <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadrDa
taQuality>
                    </oadr:oadrReportPayload>
                  </ei:interval>

                </strm:intervals>
                <ei:eiReportID>Order:LD;FRC:1;Intervals:4;ESAID:ESA#1</ei:eiReport
ID>
                <ei:reportRequestID>reportRequest_1234</ei:reportRequestID>
                <ei:reportSpecifierID>reportSpecifierID_1234</ei:reportSpecifierID
>
                <ei:reportName>x-FLEX_FORECAST</ei:reportName>
                <ei:createdDateTime>2020-10-11T23:59:27Z</ei:createdDateTime>
            </oadr:oadrReport>

            <!-
- **** FORECAST PROFILE, IO, FREQU RESP CAP=0, 4X INTERVALS, FROM ESA#1  **** --
>
            <oadr:oadrReport>
                <!-- **** Start time  **** -->
                <xcal:dtstart>
                  <xcal:date-time>2020-10-11T00:47:27Z</xcal:date-time>
                </xcal:dtstart>

                <strm:intervals>
                  <ei:interval>
                    <xcal:duration>
                       <xcal:duration>PT20S</xcal:duration>
                    </xcal:duration>
                    <oadr:oadrReportPayload>
                     <ei:rID>x-Nominal_Power</ei:rID>
                     <ei:payloadFloat>
                        <ei:value>2.0</ei:value>
                      </ei:payloadFloat>
                      <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
DataQuality>
                    </oadr:oadrReportPayload>
                  </ei:interval>

                  <ei:interval>
                    <xcal:duration>
                       <xcal:duration>PT30S</xcal:duration>
                    </xcal:duration>
                    <oadr:oadrReportPayload>
                     <ei:rID>x-Nominal_Power</ei:rID>
                     <ei:payloadFloat>
                        <ei:value>4000.0</ei:value>
                      </ei:payloadFloat>
                      <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
DataQuality>
                    </oadr:oadrReportPayload>
                  </ei:interval>

                  <ei:interval>
                    <xcal:duration>
                       <xcal:duration>PT45M</xcal:duration>
                    </xcal:duration>
                    <oadr:oadrReportPayload>
                     <ei:rID>x-Nominal_Power</ei:rID>
                     <ei:payloadFloat>
                        <ei:value>1000.0</ei:value>
                      </ei:payloadFloat>
                      <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
DataQuality>
```

Figure G.3 – Listing #3: (see Figs G.1 and G.2) Example CEM oadrUpdateReport payload *(continued)*

```
                    </oadr:oadrReportPayload>
                  </ei:interval>

                  <ei:interval>
                    <xcal:duration>
                      <xcal:duration>PT15M</xcal:duration>
                    </xcal:duration>
                    <oadr:oadrReportPayload>
                    <ei:rID>x-Nominal_Power</ei:rID>
                    <ei:payloadFloat>
                        <ei:value>600.0</ei:value>
                    </ei:payloadFloat>
                    <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadrDa
taQuality>
                    </oadr:oadrReportPayload>
                  </ei:interval>

                </strm:intervals>
                <ei:eiReportID>Order:IO;FRC:0;Intervals:4;ESAID:ESA#1</ei:eiReport
ID>
                <ei:reportRequestID>reportRequest_1234</ei:reportRequestID>
                <ei:reportSpecifierID>reportSpecifierID_1234</ei:reportSpecifierID
>
                <ei:reportName>x-FLEX_FORECAST</ei:reportName>
                <ei:createdDateTime>2020-10-11T23:59:27Z</ei:createdDateTime>
            </oadr:oadrReport>

        <!-
- **** FORECAST PROFILE, MD, FREQU RESP CAP=2, 4X INTERVALS, FROM ESA#1  **** --
>
            <oadr:oadrReport>
                <!-- **** Start time  **** -->
                <xcal:dtstart>
                  <xcal:date-time>2020-10-11T02:30:27Z</xcal:date-time>
                </xcal:dtstart>

                <strm:intervals>
                  <ei:interval>
                    <xcal:duration>
                       <xcal:duration>PT20M</xcal:duration>
                    </xcal:duration>
                    <oadr:oadrReportPayload>
                     <ei:rID>x-Nominal_Power</ei:rID>
                     <ei:payloadFloat>
                        <ei:value>40.0</ei:value>
                      </ei:payloadFloat>
                      <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
DataQuality>
                    </oadr:oadrReportPayload>
                  </ei:interval>

                  <ei:interval>
                    <xcal:duration>
                       <xcal:duration>PT3M</xcal:duration>
                    </xcal:duration>
                    <oadr:oadrReportPayload>
                     <ei:rID>x-Nominal_Power</ei:rID>
                     <ei:payloadFloat>
                        <ei:value>700.0</ei:value>
                      </ei:payloadFloat>
                      <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
DataQuality>
                    </oadr:oadrReportPayload>
                  </ei:interval>

                  <ei:interval>
```

Figure G.3 – Listing #3: (see Figs G.1 and G.2) Example CEM oadrUpdateReport payload *(continued)*

```
238.                    <xcal:duration>
239.                       <xcal:duration>PT50S</xcal:duration>
240.                    </xcal:duration>
241.                    <oadr:oadrReportPayload>
242.                     <ei:rID>x-Nominal_Power</ei:rID>
243.                     <ei:payloadFloat>
244.                        <ei:value>100.0</ei:value>
245.                     </ei:payloadFloat>
246.                     <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
    DataQuality>
247.                    </oadr:oadrReportPayload>
248.                  </ei:interval>
249.
250.                  <ei:interval>
251.                    <xcal:duration>
252.                      <xcal:duration>PT35M</xcal:duration>
253.                    </xcal:duration>
254.                    <oadr:oadrReportPayload>
255.                    <ei:rID>x-Nominal_Power</ei:rID>
256.                    <ei:payloadFloat>
257.                        <ei:value>70.0</ei:value>
258.                    </ei:payloadFloat>
259.                    <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadrDa
    taQuality>
260.                    </oadr:oadrReportPayload>
261.                  </ei:interval>
262.
263.                </strm:intervals>
264.                <ei:eiReportID>Order:MD;FRC:2;Intervals:4;ESAID:ESA#1</ei:eiReport
    ID>
265.                <ei:reportRequestID>reportRequest_1234</ei:reportRequestID>
266.                <ei:reportSpecifierID>reportSpecifierID_1234</ei:reportSpecifierID
    >
267.                <ei:reportName>x-FLEX_FORECAST</ei:reportName>
268.                <ei:createdDateTime>2020-10-11T23:59:27Z</ei:createdDateTime>
269.            </oadr:oadrReport>
270.
271.        <!-
    - **** FORECAST PROFILE, OPTIONAL#1, FREQU RESP CAP=2, 4X INTERVALS, FROM ESA#1
    **** -->
272.            <oadr:oadrReport>
273.                <!-- **** Start time  **** -->
274.                <xcal:dtstart>
275.                  <xcal:date-time>2020-10-11T01:05:00Z</xcal:date-time>
276.                </xcal:dtstart>
277.
278.                <strm:intervals>
279.                  <ei:interval>
280.                    <xcal:duration>
281.                       <xcal:duration>PT17M</xcal:duration>
282.                    </xcal:duration>
283.                    <oadr:oadrReportPayload>
284.                     <ei:rID>x-Nominal_Power</ei:rID>
285.                     <ei:payloadFloat>
286.                        <ei:value>61.0</ei:value>
287.                     </ei:payloadFloat>
288.                     <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
    DataQuality>
289.                    </oadr:oadrReportPayload>
290.                  </ei:interval>
291.
292.                  <ei:interval>
293.                    <xcal:duration>
294.                       <xcal:duration>PT18M</xcal:duration>
295.                    </xcal:duration>
296.                    <oadr:oadrReportPayload>
```

Figure G.3 – Listing #3: (see Figs G.1 and G.2) Example CEM oadrUpdateReport payload *(continued)*

```
297.                    <ei:rID>x-Nominal_Power</ei:rID>
298.                    <ei:payloadFloat>
299.                       <ei:value>40.0</ei:value>
300.                    </ei:payloadFloat>
301.                    <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
    DataQuality>
302.                  </oadr:oadrReportPayload>
303.                </ei:interval>
304.
305.                <ei:interval>
306.                  <xcal:duration>
307.                     <xcal:duration>PT67m</xcal:duration>
308.                  </xcal:duration>
309.                  <oadr:oadrReportPayload>
310.                    <ei:rID>x-Nominal_Power</ei:rID>
311.                    <ei:payloadFloat>
312.                       <ei:value>1000.0</ei:value>
313.                    </ei:payloadFloat>
314.                    <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadr
    DataQuality>
315.                  </oadr:oadrReportPayload>
316.                </ei:interval>
317.
318.                <ei:interval>
319.                  <xcal:duration>
320.                    <xcal:duration>PT35M</xcal:duration>
321.                  </xcal:duration>
322.                  <oadr:oadrReportPayload>
323.                  <ei:rID>x-Nominal_Power</ei:rID>
324.                  <ei:payloadFloat>
325.                      <ei:value>45.0</ei:value>
326.                  </ei:payloadFloat>
327.                  <oadr:oadrDataQuality>Quality Good - Non Specific</oadr:oadrDa
    taQuality>
328.                  </oadr:oadrReportPayload>
329.                </ei:interval>
330.
331.              </strm:intervals>
332.              <ei:eiReportID>Order:1;FRC:2;Intervals:4;ESAID:ESA#1</ei:eiReportI
    D>
333.              <ei:reportRequestID>reportRequest_1234</ei:reportRequestID>
334.              <ei:reportSpecifierID>reportSpecifierID_1234</ei:reportSpecifierID
    >
335.              <ei:reportName>x-FLEX_FORECAST</ei:reportName>
336.              <ei:createdDateTime>2020-10-11T23:59:27Z</ei:createdDateTime>
337.            </oadr:oadrReport>
338.
339.        <ei:venID>venID>venID _54342</ei:venID>
340.        </oadr:oadrUpdateReport>
341.        </oadr:oadrSignedObject>
342.        </oadr:oadrPayload>
```

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 60364-8-3, *Low-voltage electrical installations – Functional aspects — Operation of prosumer's electrical installations*

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 1879:2021, *Energy smart appliances – Demand side response operation – Code of practice*

prEN50491-12-2 (in preparation)

Other publications

[1] GREAT BRITAIN. Electricity Act 1989. London: The Stationery Office

[2] GREAT BRITAIN. The Measuring Instruments Regulations 2016. London: The Stationery Office

[3] ELEXON. *Balancing and Settlement Code*. [Available at https://www.elexon.co.uk/bsc-and-codes/bsc-related-documents/codes-of-practice/]

[4] ELEXON. *Profiling*. [Available at https://www.elexon.co.uk/operations-settlement/profiling/]

[5] DEPARTMENT OF BUSINESS, ENERGY AND INDUSTRIAL STRATEGY, *Smart Meter Communication Licence*. [Available at https://epr.ofgem.gov.uk/Content/Documents/Smart%20DCC%20Limited%20-%20Smart%20Meter%20Communication%20Consolidated%20Licence%20Conditions%20-%20Current%20Version.pdf]

[6] ZIGBEE ALLIANCE. *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]

[7] GREAT BRITAIN. Data Protection Act 2018. London: The Stationery Office

[8] SMART ENERGY CODE. Smart Metering Implementation Programme: Smart Metering Equipment Technical Specifications Version 2. SEC, 2020 [Available at: http://www.smartenergycodecompany.co.uk/download/29586] (last accessed 30 March 2021)

[9] SMART ENERGY CODE. Smart Metering Implementation Programme: Great Britain Companion Specification (GBCS) version 4.0. SEC, 2020. [Available at: https://smartenergycodecompany.co.uk/download/29602] (last accessed 30 March 2021)

[10] DATA COMMUNICATIONS COMPANY. *User interface specification*. [Available at: https://www.smartdcc.co.uk/document-centre/interface-specifications/dcc-user-interface-specification/]

[11] SMART ENERGY CODE. *Technical and Business Architecture Documents*.[Available at https://smartenergycodecompany.co.uk/the-business-architecture-document-bad/]

[12] DATA COMMUNICATIONS COMPANY. *DCC User roles*. [Available at: https://www.smartdcc.co.uk/customer-hub/about-dcc-users/]

[13] SMART ENERGY CODE. *Security and privacy obligations overview*. [Available at: https://smartenergycodecompany.co.uk/about-security-and-privacy-obligations]

[14] SMART ENERGY CODE. *Communications Hubs Technical Specification*. [Available at https://smartenergycodecompany.co.uk/glossary/communications-hub-technical-specification/] (last accessed 23 March 2021)

[15] DEPARTMENT OF ENERGY AND CLIMATE CHANGE. *Smart Metering Equipment Technical Specifications*. 2014. [Available at https://www.gov.uk/government/consultations/smart-metering-equipment-technical-specifications-second-version]

[16] OPENADR ALLIANCE. *OpenADR 2.0 Profile Specification*. copyright 2011-2012. [Available at https://www.openadr.org/specification]

[17] OPENADR ALLIANCE. *OpenADR 2.0 Demand Response Program Implementation Guide, v1.p*, July 2014. [Available at https://www.openadr.org/assets/openadr_drprogramguide_v1.0.pdf]

Further reading

CENELEC EN50631-1:2017, *Household appliances network and grid connectivity. General Requirements, Generic Data Modelling and Neutral Messages.*

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).*

European Commission, *Study on ensuring interoperability for enabling Demand Side Flexibility*. Published 2018, ISBN 978-92-79-91255-9.

ETSI TS 103 264 V1.1.1 SmartM2M; *Smart Appliances; Reference Ontology and oneM2M Mapping*.

ETSI TS 103 410-1 V1.1.1 SmartM2M; *Smart Appliances Extension to SAREF; Part 1: Energy Domain*.

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).

FlexiblePower Alliance Network (FAN). *Energy Flexibility Interface* (EFI). Available at https://flexible-energy.eu/efi-energy-flexibility-interface/

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards-based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email cservices@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Relations
Tel: +44 345 086 9001
Email: cservices@bsigroup.com

Subscription Support
Tel: +44 345 086 9001
Email: subscription.support@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com