PAS 1879:2021

Energy smart appliances – Demand side response operation – Code of practice

Department for Business, Energy & Industrial Strategy

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2021.

ISBN 978 0 539 05130 8

ICS 03.100.70; 27.015; 91.140.50; 97.100

Publication history

First published May 2021

Contents

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 Hugh Boyes of Bodvoc Ltd, as the technical author, and the organizations that were involved in the development of this PAS as members of the steering group:

- Association for Decentralised Energy (ADE)
- Association of Manufacturers of Domestic Appliances (AMDEA)
- BEIS/OZEV
- British Electrotechnical and Allied Manufacturers' Association (BEAMA)
- Carbon Co-op
- Consumer and Public Interest Network (CPIN)
- EDF
- Energy Networks Association (ENA)
- Energy Systems Catapult
- Flexitricity
- Kiwi Power
- Landis+Gyr
- Moixa Technology Ltd
- National Grid ESO
- Northern Powergrid
- Ofgem
- OVO Energy/Kaluza
- Schneider Electric
- Western Power Distribution

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

This PAS is not to be regarded as a British Standard. It will be withdrawn in the event it is superseded by a British Standard.

The PAS process enables a code of practice 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

It is intended that this PAS is read in conjunction with PAS 1878:2021, which addresses the operation of energy smart appliances (ESAs). Demand side response operation of ESAs defined within this PAS does not require the use of a smart metering system but is nevertheless compatible with smart metering systems.

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

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

As a code of practice, this PAS takes the form of recommendations and guidance. It is not to be quoted as if it were a specification. Users are expected to ensure that claims of compliance are not misleading.

Users may substitute any of the recommendations in this PAS with practices of equivalent or better outcome. Any user claiming compliance with this PAS is expected to be able to justify any course of action that deviates from its recommendations.

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 recommendations are expressed in sentences in which the principal auxiliary verb is "should".

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

The word "should" is used to express recommendations of this PAS. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this PAS. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

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
- 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, as additional benefits might 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 services set out in this PAS and PAS 1878:2021, 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 provides guidance on the information exchange within prosuming electrical installations, e.g. IEC TS 60364-8-3:2020, Table 1.

This PAS provides recommendations for the provision of DSR services by service providers and it is intended to be read in conjunction with PAS 1878:2021, which provides a technical specification that allows domestic appliances to operate in such a DSR system.

0.2 Demand side response (DSR)

Response mode DSR requires communication between domestic appliances and a controlling entity, which itself communicates with the appropriate regulated electricity market participants. 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.

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 meet the requirements specified in PAS 1878:2021. In the concept of operation recommended in this PAS, the ESA provides information to the DSRSP with options regarding how it is able to modulate its power requirements over time – its power "flexibility" – over a communications interface.

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. 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 provided in PAS 1878:2021, Annex C.

This PAS provides minimum recommendations for functionality, information flow, communications capability and cyber security for the implementation of a DSR service. These minimum recommendations ensure a sufficient level of interoperability, security and optionality whilst not limiting the opportunity for product and service innovation. An overview of DSR service provision is set out in **4.3**.

0.3 Energy smart appliances and the DSR functional architecture

ESAs currently covered in this PAS include domestic smart EV chargepoints, electrically powered HVAC, battery storage, wet appliances and cold appliances, but the ESA classification is not limited to these appliances; if an appliance not listed meets the specification in PAS 1878:2021 it can be considered an ESA. The technical requirements an ESA will need to meet in order to provide DSR services are specified in PAS 1878:2021.

In order to support a minimum level of DSRSP and ESA interoperability for every ESA type, PAS 1878:2021 requires that each ESA is supplied with a customer energy manager (CEM). 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.

Functionality in addition to that offered by these ESAs, such as communications gateway functionality, depicted as an "Energy Gateway", is also required in an end-to-end DSR system and is treated in this PAS as a necessary component of the entire system. This PAS addresses the principles set out in **0.5** in terms of two functional architectures as illustrated in Figure 1 and Figure 2, which represent instances of in-home and cloud-based combined CEM respectively. The functionality of the CEM is described further in PAS 1878:2021, Annex E.

The Energy Gateway represents the physical communications device that provides the logical connectivity between the in-premises elements of the DSR architecture and those elements located outside the premises, as illustrated in Figure 1 and Figure 2. The connectivity between the Energy Gateway at a premises and a DSRSP may be wired (e.g. broadband) or wireless (e.g. 4G, 5G, LPWAN, etc.).

NOTE 1 *If the connection to the premises is provided via the internet, the Energy Gateway is represented by the broadband modem/router. In this scenario, a key feature of the Energy Gateway is its firewall, which limits access to in-premises network to traffic that is in accordance with the firewall rules. Given the presence of a firewall, the initiation of communications between an ESA and the DSRSP occurs from inside the premises, as attempts by an external IP address to initiate a connection to a device in the premises would normally be blocked by the firewall. In scenarios where alternative wireless communications channels are employed, the Energy Gateway might, for example, be a GSM modem.*

Figure 1 – DSR architecture – in home

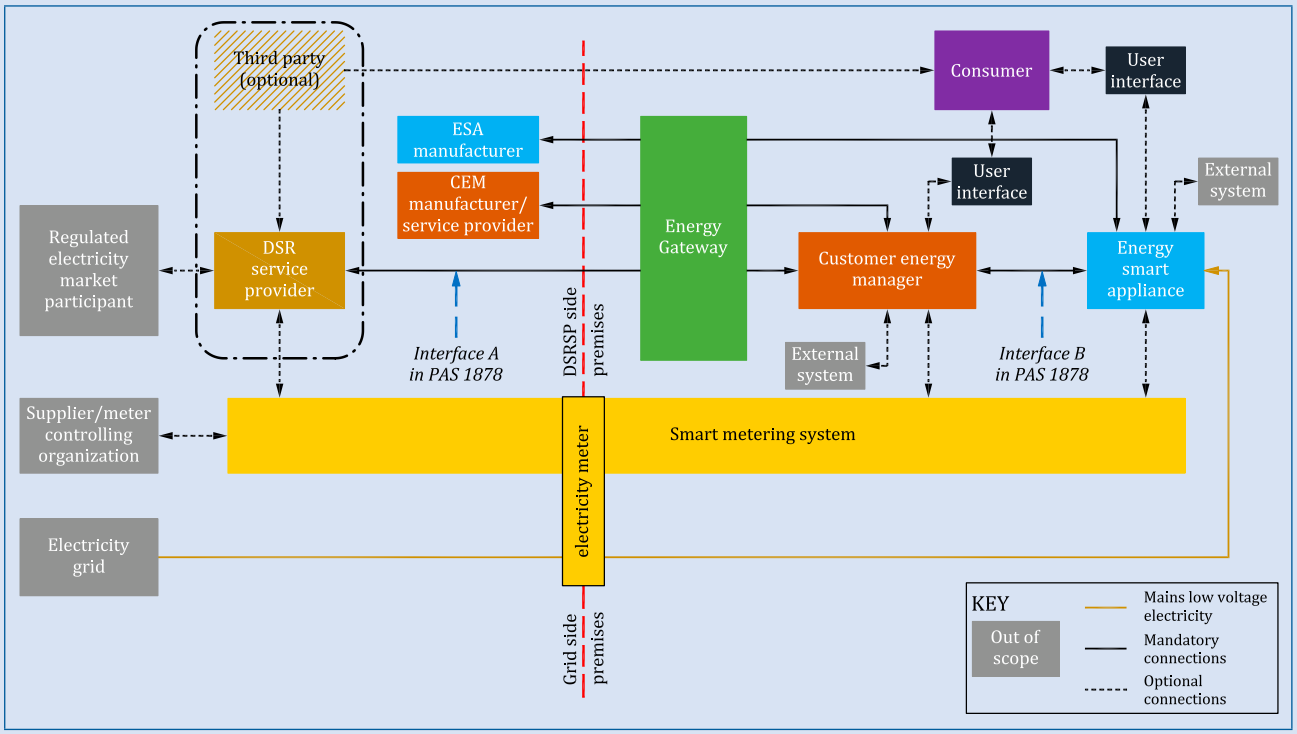
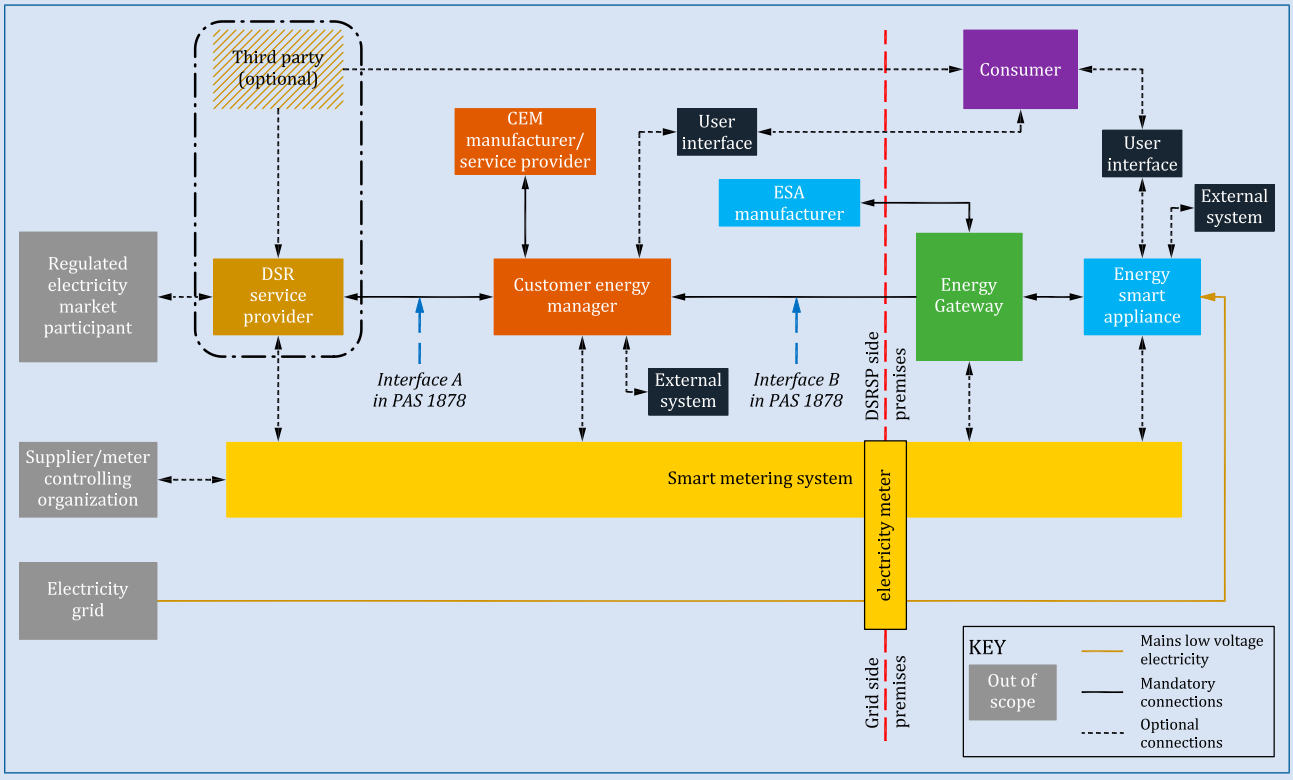


Figure 2 – DSR architecture – cloud-based CEM



NOTE 2 *In Figure 1 and Figure 2 the user interfaces are shown as optional to accommodate the variety of ways in which a consumer can connect to the ESA and set their preferences in the CEM. The specific requirements for user interface provision are described in PAS 1878:2021. Consumer preferences and consent are necessary features of DSR but the specific means by which a user interface is provided is a design issue for ESA manufacturers and DSRSPs.*

NOTE 3 *The functional architectures illustrated in Figure 1 and Figure 2 are based on the CENELEC and IEC architectures illustrated in PAS 1878:2021, Annex E. The figures are intentionally more detailed than those in PAS 1878:2021 as they are intended to show the relationships between different elements of an overall DSR architecture. They are non-exhaustive illustrations of DSR functional implementations employing in-home and cloud-based CEMs respectively. Other approaches can equally deliver the four principles in* ***0.5****.*

NOTE 4 *Delivery of DSR services through a smart meter system will depend on national implementation of smart metering. PAS 1878:2021, Annex D, illustrates this for the GB smart metering system through the use of auxiliary proportional controllers (APCs) and standalone auxiliary proportional controllers (SAPCs).*

NOTE 5 *In Figure 1 and Figure 2, the optional third party shown between the consumer and the DSRSP is intended to cover business scenarios where the DSRSP does not deal directly with consumers; for example, where the third party provides consumer recruitment and consumer relationship management services.*

NOTE 6 *Where a DSRSP contracts or works with third parties to operate part of the DSR service on its behalf, the DSRSP retains full and final responsibility for appropriate delivery of all services whether sub-contracted or not. This includes the optional third party referred to in Note 5. In the architectures illustrated in Figure 1 and Figure 2, where a third party provides the CEM, the DSRSP retains responsibility for the end-to-end security of the DSR service.*

0.4 Operational model

COMMENTARY ON ***0.4***

A DSRSP may sub-contract the provision of aggregated DSR services to a third party. In this case, the sub-contracted third party maintains an up-to-date list of flexibility options for each ESA and provides an up-to-date summary of the technical capability to the DSRSP as requested. The DSRSP remains responsible for all the recommendations in this PAS being met by the sub-contracted third party providing the DSR service, as described in ***4.3.10****.*

Following the subscription to, and set up of, a DSR service for an individual ESA, the DSR system operates in the following manner (see also PAS 1878:2021, Figure 2).

a) The ESA determines its flexibility options (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 PAS 1878:2021.

   NOTE 1 *A flexibility option represents the ability of the ESA to vary its demand or supply of electricity over a defined period. Where the ESA is working through a planned/programmed cycle of energy use, a flexibility option can be to delay or increase demand over the next phase of the programmed cycle.*

   NOTE 2 *Where a CEM is connected to more than one ESA it can present flexibility options as a composition of the options jointly and individually available from the ESAs.*

b) This information is updated whenever the flexibility status of the ESA changes (e.g. the consumer turns the ESA on or off) or a flexibility option is no longer valid (e.g. it has expired or has 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 options. The ESA implements this flexibility option and enters response mode.

f) During the DSR event period:

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

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

   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 may 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 that requested the DSR service (including real-time power consumption values).

NOTE 3 *The above interactions are covered in more detail in PAS 1878:2021, which also describes how interoperability between DSRSPs and ESAs is supported by the use of a common format describing energy flexibility options and standardized interface communication protocols.*

0.5 Alignment with DSR and ESA principles

Four principles are seen as critical for effective DSR through ESAs. This PAS aligns with these principles as listed below and explained in Clause **5**.

- **Interoperability**
  The ability of an ESA to work seamlessly across any appropriate DSR service operated by any DSRSP.
- **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 unexpected or 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.

0.6 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 PAS 1878:2021, 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.*

0.7 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 work carried out in several CEN/CENELEC and ISO/IEC Technical Committees, including IEC TC 57, *Power systems management and associated information exchange*; CLC TC 205, *Home and building electronic systems*; and CENELEC TC59X, *Performance of household and similar electrical appliances*.

Details of specific standards to be applied to the structure, format and contents of messages between the DSRSP and consumers' premises are outlined in PAS 1878:2021.

1 Scope

1.1 In scope

This PAS sets out a common definition of demand side response (DSR) services for actors operating within the consumer energy supply chain and provides recommendations to support the operation of energy smart appliances (ESAs). The consumer-focused approach outlined in this PAS can coexist with other forms of balancing or DSR.

NOTE 1 *Regulated market participants currently use a range of balancing services. This PAS is not intended to limit or replace the operation of other forms of balancing or demand management, which fall outside the scope of this PAS and PAS 1878:2021; for example, DSR regarding larger industrial and commercial electricity users.*

This PAS is aimed at those organizations responsible for providing and delivering energy services to domestic (e.g. individual households) or small business (i.e. SME) premises, which are collectively referred to as consumers. The cyber security principles in this PAS apply to organizations performing any form of DSR, or sending remote signals to appliances to shift or modulate their energy consumption or supply.

With regards to compatibility with all forms of DSR-based activity, the two types of consumer DSR covered by this PAS are those employing ESAs, compliant with the specification in PAS 1878:2021, that implement:

a) routine DSR implemented through supplier set electricity tariffs or other electricity-related incentives; and/or

b) response DSR initiated at the request, often made in near real time, of regulated electricity market participants.

This PAS provides only the minimum recommendations to perform DSR-based activities involving electrical appliances used in domestic or small business settings. The specific appliance categories in scope for domestic DSR service are:

1) heating, ventilation and air conditioning appliances (HVAC);

2) cold appliances;

3) wet appliances;

4) battery storage; and

5) smart EV chargepoints.

NOTE 2 *Any other type of appliance which meets specifications set out in PAS 1878:2021 can be considered an ESA.*

1.2 Out of scope

Aspects out of scope for this PAS are the:

a) functional and non-functional requirements of an ESA;

NOTE 1 *Product safety of ESAs in respect of their energy smart functionality is addressed in PAS 1878:2021.*

b) commercial models of DSR;

c) ethics and social rules of DSR operation;

d) contracting, payment services or general consumer protections; and

NOTE 2 *Whilst these aspects of service delivery are out of scope of this PAS, adoption and implementation of good industry practices by DSRSPs regarding interaction with and treatment of consumers is a reasonable consumer expectation.*

e) curtailment of supply.

1.3 Intended audience for this PAS

This PAS is intended for use by all actors operating within the domestic energy supply chain, including transmission system operators (TSOs), distribution network/system operators (DNOs) and electricity suppliers and aggregators. It might also be of interest to manufacturers of ESAs and customer energy managers (CEMs). Other parties who might have an interest in this PAS are maintainers of ESAs, manufacturers and maintainers of interfacing products, software developers and other service providers.

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. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies[1)].

Standards publications

ETSI EN 303 645, *Cyber security for consumer internet of things: Baseline requirements*

IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*[2)]

IEC TS 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

PAS 1878:2021, *Energy smart appliances – System functionality and architecture – Specification*

[1)] Documents that are referred to solely in an informative manner are listed in the Bibliography.
[2)] At the time of publication, BS EN IEC 62443-2-1 is in preparation and is expected to be published in due course.

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 aggregator

service provider that manages electrical energy demand (consumption) or export (production) on behalf of a group of consumers

3.1.2 appliance

product or system that consumes, stores, exports and/or generates electrical energy during its functional use

NOTE *Some appliances might have hybrid functionality; for example, an EV can both store electrical energy and use it to provide mobility services.*

3.1.3 asset

item, thing or entity that has potential or actual value to an individual, an organization or a government

NOTE *An asset can be fixed, mobile or movable. It can be an individual item, plant, a system of connected equipment, a space within a structure, a piece of land, an entire piece of infrastructure, an entire building, or a portfolio of assets. An asset might also comprise data or information in digital or in printed form, as well as an organization's internal processes.*

Digital information can be localized (i.e. based on a single data source) or distributed (i.e. derived from multiple data sources and/or locations).

The value of an asset might vary throughout its life and an asset might still have value at the end of its life. Value can be tangible, intangible, financial and non-financial.

3.1.4 certificate organization

entity that certifies the ownership of a public key by the named subject of a digital certificate

3.1.5 consumer

domestic (i.e. individual households) or small business user (i.e. SME) who:

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

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

3.1.6 consumer's authorized representative

individual who has been been appointed, formally or informally, to act on behalf of a consumer in a vulnerable situation

NOTE 1 *The representative might be a partner, family member, carer, social worker or health professional.*

NOTE 2 *Attention is drawn to applicable national or regional laws that relate to the formal appointment of a representative, the representative's mandate, and how matters relating to privacy and data protection are managed by those acting on instructions from the representative.*

3.1.7 customer energy manager (CEM)

logical entity providing functionality used to manage one or more ESAs, specific to a supply point, in order to provide DSR service

NOTE 1 *PAS 1878:2021 specifies that an ESA manufacturer will supply a CEM with every ESA. Where an ESA manufacturer contracts a third party to deliver the CEM functionality the requirements of PAS 1878:2021 still apply.*

NOTE 2 *A CEM could either be in an interface box located in the premises or in the cloud with connectivity to the ESA.*

NOTE 3 *In this PAS, the term "CEM" indicates a CEM/ESAG combination or an individual CEM, as appropriate, unless otherwise stated.*

3.1.8 cyber hygiene

practices that users of computers and digital systems can take to maintain system health, improve online security and reduce the risk of data loss or corruption

3.1.9 data and information sharing agreement (DISA)

documented and agreed policy, process, procedures and remedies in respect of data shared between a data owner and another party or parties

3.1.10 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

3.1.11 demand side response service provider (DSRSP)

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

3.1.12 Energy Gateway

communications bridge between DSR-related devices located inside and outside the consumer's premises

NOTE *Where a DSR service uses the internet as the communications channel between the DSRSP and an ESA, the consumer's broadband router would be the Energy Gateway.*

3.1.13 energy smart appliance (ESA)

appliance which is communications-enabled and able to respond automatically to price and/or other signals by shifting or modulating its electricity consumption and/or production

NOTE *ESAs referenced in this PAS are those compliant with the requirements in PAS 1878:2021, and unless explicitly referred to in the text the term ESA is taken to include the associated CEM functionality irrespective of how this is delivered.*

3.1.14 heating, ventilation and air conditioning (HVAC) appliances

electrical goods used in domestic or small business environments for heating, ventilation or air conditioning

3.1.15 interoperability

ability of an ESA, and its associated CEM, to work seamlessly across any appropriate DSR service operated by any DSRSP, including allowing a consumer to switch an ESA to a different DSRSP at any time and maintain DSR functionality

3.1.16 national regulatory authority

entity appointed as a national authority to oversee the operation of the electricity market and responsible for establishing and maintaining the regulatory framework for electricity generation, transmission, distribution and supply

NOTE *A national regulatory authority has the ability to delegate responsibilities to other entities it regulates.*

3.1.17 personal data

information relating to an identified or identifiable living individual

[SOURCE: Data Protection Act 2018, Section 1(2)] [4]

NOTE 1 *This term is also defined in the General Data Protection Regulation (GDPR) [5].*

NOTE 2 *In a DSR context, in addition to the categories covered in the Data Protection Act 2018 [4], personal data will include any unique identifiers assigned to a consumer's account, premises, metering point, CEM, ESAG and ESA(s).*

3.1.18 premises

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

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

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

3.1.19 premises area network

network within a premises to which a consumer's communications-enabled devices and appliances are connected

NOTE *A premises area network can be a combination of wired and/or wireless connections that connect to the public network(s) via an Energy Gateway.*

3.1.20 registration organization

entity responsible for assessing whether a potential DSRSP meets any criteria set by the national regulatory authority for approval of service delivery within the regulator's jurisdiction

NOTE *The need for DSRSP approval and any criteria a potential DSRSP meets is determined by the relevant national regulatory authority. The entity may be the national regulatory authority or another entity appointed by the national regulatory authority to provide the approval service.*

3.1.21 regulated electricity market participant

organization operating within a regulated electricity market to provide services which can include generation, transmission, distribution and balancing activities

NOTE *The regulated electricity market participants who initiate DSR interventions would at a minimum be the transmission system operator (TSO), distribution network operators (DNOs) and suppliers, but may include other participants authorized by the national regulatory authority.*

3.1.22 security

state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts

3.1.23 smart EV chargepoint

"energy smart" equipment enabling the recharging, or in the case of V2G discharging, of an EV

NOTE *The "energy smart" aspect of this definition is referring to a chargepoint that meets the specification for an ESA as set out in PAS 1878:2021.*

3.1.24 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 *See also the latest versions of SMETS (and GBCS) and the DCC user interface specification*[3)]*.*

3.1.25 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)

3.1.26 vendor lock-in

use of mechanisms or protocols by a vendor to prevent interoperability of the energy smart features of an ESA

3.2 Abbreviated terms

CEM	customer energy manager
CISP	cyber information sharing platform
DCC	data communications company
DISA	data and information sharing agreement
DNO	distribution network operator
DSR	demand side response
DSRSP	demand side response service provider
ESA	energy smart appliance
ESAG	ESA Gateway
ESO	electricity system operator
HAN	home area network
HTTPS	hypertext transfer protocol secure
HVAC	heating ventilation and air conditioning
SME	small and medium-size enterprise
TLS	transport layer security
ToU	time of use
TSO	transmission system operator
V2G	vehicle to grid

[3)] Available at: https://smartenergycodecompany.co.uk/the-smart-energy-code-2/.

4 Actors in consumer DSR

*COMMENTARY ON CLAUSE **4***

Within this PAS, ESA is a defined term, which means the asset is compliant with PAS 1878:2021.

4.1 Transmission system operator (TSO)

*COMMENTARY ON **4.1***

In Great Britain, the TSO is referred to as the ESO, a role undertaken by the National Grid ESO. The TSO develops and delivers the short-term electricity transmission plan, i.e. forecasting supply and demand, and operating the electricity network in real time to maintain the security, quality and stability of the electricity transmission network. As part of its portfolio of balancing services, the TSO can elect to make use of services from a DSRSP to manage any mismatch between supply and demand on the network.

When the TSO requires a DSR intervention to manage the operation of the transmission network, it should only request such interventions from DSRSPs that:

a) where required by the national regulatory authority have sought and maintained approval to provide consumer DSR services; and

b) employ a valid digital certificate signed by a trusted certificate organization for all communications with consumers and ESAs.

In requesting a balancing intervention, the TSO should specify to the DSRSP the required parameters for the intervention, which should include:

1) the start time of the intervention;

2) the duration of the intervention (where applicable);

3) the magnitude of the required change in load or generation; and

4) any geographical constraints, i.e. a target part of the transmission network.

4.2 Distribution network operator (DNO)

*COMMENTARY ON **4.2***

The DNO is responsible for the distribution of electricity from the interface between the high voltage electricity transmission system (operated by the TSO) and their regional network, through the regional and local networks to individual premises level (consumer) metering points. In addition, the DNO is responsible for carrying energy from generators embedded in its network and/or to and from energy storage systems within its network to either the interface with the TSO system, or to industrial and domestic consumers connected to its network.

The traditional distribution model is focused on the one-way flow and delivery of electricity, with clear and reliable definitions of upstream (i.e. connectivity to the TSO system) and downstream (connections to consumers' premises). The introduction of distributed generation, renewable sources (e.g. solar farms and wind farms), energy storage and microgrids is changing the operation of the distribution network. Rather than managing an unidirectional model of electricity delivery, the DNOs are becoming operators of a more complex, systemic model and account for and manage multiple points of variable supply and consumption.

The DNO is responsible for maintaining the quality of the electricity distributed within its network and for managing constraints in its network so as to maintain network integrity. DNOs might elect to make use of services from a DSRSP to:

a) manage constraints in the regional network (i.e. between TSO supply point and DNO substation(s));

b) provide local balancing services (for example at a substation) where peak energy demand is likely to outstrip local energy supply or the capacity of the local network; and

c) undertake any other purpose identified by the network operator, e.g. managing network loads or improving network reliability.

In the drafting of this PAS, the term DNO has been used to represent the organization responsible for the operation of the distribution network. In some jurisdictions the term distribution system operator (DSO) can be used to cover these operational activities.

When the DNO requires a DSR intervention to manage the stability of the distribution network, it should only request such interventions from DSRSPs that:

a) where required by the national regulatory authority have sought and maintained approval to provide consumer DSR services; and

b) employ a valid digital certificate signed by a trusted certificate organization for all communications with consumers and ESAs.

In requesting a DSR intervention, the DNO should specify to the DSRSP the required parameters for the intervention, which should include:

1) the start time of the intervention;

2) the duration of the intervention (where applicable);

3) the magnitude of the required change in load or generation or the level which the load or generation should be below/above; and

4) any geographical constraints, i.e. a target part of the distribution network.

4.3 DSR service providers (DSRSP)

4.3.1 Compliance with PAS 1878:2021

When operating ESAs for DSR, the DSRSP should construct its system in accordance with the requirements set out in PAS 1878:2021.

4.3.2 Approval to provide consumer DSR services

In jurisdictions where the national regulatory authority requires DSRSPs to be approved:

a) an organization intending to provide consumer DSR services should consult with the national regulatory authority for the jurisdiction where it plans to deliver the services;

b) where the national regulatory authority requires an application to be submitted for approval (see **4.6**) the DSRSP should seek approval before commencing delivery of consumer DSR services; and

c) in the event that a DSRSP ceases to be approved, it should cease delivery of consumer DSR services.

NOTE 1 *The approval to provide consumer DSR services might be for a specified period and might require the organization to demonstrate that specified criteria continue to be met.*

NOTE 2 *The national regulatory authority may use a registration organization to assess potential DSRSPs.*

4.3.3 DSR digital certificate

Before commencing operation as a DSRSP, the organization should obtain a digital certificate signed by a trusted public certificate organization. A DSRSP should not use a self-certified digital certificate to secure the communications between the DSRSP and ESAs.

NOTE 1 *The digital certificate is intended to be used to sign and encrypt data sent by the DSR to ESAs. In signing a standard digital certificate, the certificate organization is guaranteeing the information in the certificate, but is making no claims about the competence or security of the entity, in this case the DSRSP, that owns the certificate.*

NOTE 2 *Examples of commonly trusted certificate organizations include Comodo SSL, RapidSSL, Thawte SSL, GeoTrust SSL and Symantec SSL. The organizations are commonly referred to as certificate authorities.*

4.3.4 General roles and responsibilities in delivering consumer DSR

Where a DSRSP provides consumer DSR services to the TSO and/or DNO, this should be done using a portfolio of ESAs, where consumers and other entities (e.g. third parties such as operators of EV chargepoints) have made the ESAs available to the DSRSP as part of a service agreement.

NOTE *The nature of the DSR service offered to the TSO and/or DNO depends on the responsiveness of the communications network between the DSRSP and ESAs, and the capabilities of consumers' ESAs.*

4.3.5 Security related roles and responsibilities in delivering consumer DSR

Given the potential impact of a security failure on the electricity grid and consumers, the DSRSP should demonstrate that it has adopted the holistic approach to security described in **6.2**.

4.3.6 Consumer and ESA enrolment

Before subscribing a consumer to its service, the DSRSP, or a third party contracted to act on the DSRSP's behalf, should:

a) receive and process an application from the consumer or the consumer's authorized representative;

b) check that the applicant has appropriate authority and consent to subscribe to the service; and

c) validate the information provided by the consumer, or the consumer's authorized representative, to a degree that is proportionate to the risk that incorrect information would pose to the integrity of the DSRSP's service.

Before subscribing a consumer's ESA in its service portfolio, the DSRSP should:

1) verify the trustworthiness of the ESA's configuration; and
2) test the end-to-end messaging and the correct behaviour of the ESA in response to DSR signals.

The DSRSP should perform the verification and testing required by 1) and 2) above on initial subscription of an ESA.

***NOTE** The verification might need to be periodically repeated to confirm that security updates have been applied by a subscribed ESA. For subscribed ESAs further testing might be required to investigate consumer complaints or failure of an ESA to respond to DSRSP messages.*

4.3.7 Consumer relationship management

***NOTE 1** References to an ESA in this clause include the associated CEM functionality, however this is provided, e.g. in premises or cloud-based.*

Having subscribed a consumer's appliances in its ESA portfolio, a DSRSP, or a third party contracted to act on the DSRSP's behalf, should provide a number of relationship management services to the consumer or consumer's authorized representative (as applicable). These should include, but are not limited to, allowing the consumer to:

a) opt out of DSR interventions;
b) add a new ESA;
c) remove a subscribed ESA or unenroll from the DSRSP's service (within the terms of their contract);
d) resolve situations where the ESA is not functioning appropriately; and

   ***NOTE 2** In such situations a DSRSP may declare the ESA as unavailable for the DSR services until the situation is sorted. If the situation is not resolved within a reasonable timescale, the DSRSP may remove the ESA from its ESA portfolio.*

e) move premises whilst remaining a subscriber (while also recognizing that, in some circumstances, a DSRSP might not be able to replicate the services offered to the consumer in their new location).

The DSRSP might have a contractual relationship with a third party rather than directly with the consumers; for example, an operator of smart EV chargepoints might manage the acquisition of consumers and provide the consumer relationship management services, but the DSR service interventions are called by the DSRSP. In this type of relationship, if an ESA is unsubscribed, the third party should update the DSRSP and confirm that the ESA has been removed from the DSRSP's portfolio.

Where a third party is delivering the consumer relationship management services, Clause **8** should still apply to the DSRSP in respect of any data or information it processes that is covered by the prevailing national data protection legislation or regulations.

The DSRSP should retain the service and security responsibility if a third party is contracted to deliver relationship management services.

***NOTE 3** This PAS and PAS 1878:2021 were developed under the principle of interoperability. As such, behaviour relating to the seamless switching of consumer between DSRSPs is compatible with this PAS.*

4.3.8 Implementation of DSR interventions

*COMMENTARY ON **4.3.8***

The typical DSR intervention described below is an illustrative minimum and is not to be seen as constraining intervention models. The actions below may be undertaken by the DSRSP or a third party contracted to act on the DSRSP's behalf.

A typical DSR intervention should operate in the following manner.

a) Each subscribed ESA, or collection of ESAs represented by a CEM, should provide its available flexibility options (power forecasts), individually or as combined forecasts, to the DSRSP, using the CEM and ESAG as an intermediary.

   ***NOTE 1** The CEM communicates with the DSRSP using a common interface specified in PAS 1878:2021.*

   ***NOTE 2** If the ESA is a smart EV chargepoint the flexibility may be calculated by the CEM.*

   ***NOTE 3** A DSRSP can provide augmented Interface A communications, as long as the communications provide the core mandatory Interface A messaging as specified in PAS 1878:2021.*

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

c) The DSRSP should maintain a list of the possible flexibility options for each consumer premises and subscribed ESA.

d) Whenever the DSRSP is requested to provide a DSR service, based on the required modulation and network areas affected, the DSRSP should select, from its list of ESAs and flexibility options, the portfolio of ESAs to be contacted.

e) Where the DNO, or the TSO, requests a DSR intervention targeted at a specific part of their network, the DSRSP should, based on the network location of consumers' premises that was captured as part of the consumer registration process, employ an appropriate portfolio of ESAs to deliver the intervention.

NOTE 4 *The address of a consumer's premises is not a reliable indicator of its location on a DNO's network. Where a DNO is requesting interventions targeted at specific areas of its network, it might require DSRSPs to have knowledge of and offer interventions based on the network location of an ESA rather than the address at which the ESA is installed.*

f) The DSRSP should then send a message to the selected ESAs, via their CEMs, requesting that they implement one of their provided flexibility options (the DSRSP should then receive confirmation from the selected ESAs, either that the requested flexibility option has been implemented, or that it has not).

g) Once the DSR period is completed, the ESA provides the DSRSP with information concerning its power consumption throughout the period (as described in PAS 1878:2021, **5.5**); the DSRSP should then provide aggregated flexibility information to the party requesting the DSR service.

As specified in PAS 1878:2021 with regards to Mode 3 operation of an ESA, the DSRSP should inform the consumer of any planned or current ESA/DSR flexibility operation. The DSRSP should also provide transparency for the consumer regarding the nature, frequency and duration of any DSR event for any ESAs the consumer has subscribed to the DSRSP's service.

4.3.9 Provision of flexible and scalable DSR interventions

If a DSRSP wishes to provide services on a scalable basis, it should design its systems to allow DSR interventions to operate at multiple levels. This is to maintain the aggregate demand within the capacity of the distribution network and the available electricity supply, for example, at distribution area, sub-station, street and potentially premises/site level.

From a grid security perspective, switching of aggregated loads and generation should be managed to:

a) prevent supply instability;

b) maintain transmission and distribution system resilience; and

c) prevent damage or disruption to supply equipment through excessive loads or changes in loads.

NOTE *Where multiple DSRSPs are operating within a given area, grid security depends on some coordination of their activities by the ESO and/or DNOs, so that conflicting DSR signals are not sent and their switching of aggregate loads does not jeopardize the stability and security or safety of the distribution network.*

4.3.10 Third parties acting on behalf of DSRSPs

Third parties may operate on behalf of a DSRSP to fulfil DSRSP sub-functionalities; these third parties may perform various functions and sit at various points in the DSR architecture. In all cases, the DSRSP should retain full and final responsibility for appropriate delivery of all services, including those delivered by third parties on behalf of the DSRSP.

4.4 Electricity suppliers

Where an electricity supplier wishes to facilitate or encourage consumer DSR, they should offer routine mode DSR through ToU tariffs and maintain the tariff information so it is accurate and readable by a suitably connected and configured ESA.

NOTE 1 *See PAS 1878:2021, Annex D, for further GB specific information on ESAs' reading of tariffs.*

Suppliers should not contract with DSRSPs in a manner which causes consumer lock-in or prevents interoperability of DSR services.

Suppliers contracting with the DSRSP should follow national guidance on imbalances.

NOTE 2 *As a regulated electricity market participant, an electricity supplier may be permitted to request response mode DSR interventions via DSRSPs to balance the demand for the electricity it supplies to or buys from consumers.*

NOTE 3 *If permitted by national electricity market regulations, an electricity supplier could, including, where applicable, obtaining approval, become a DSRSP. In such circumstances the supplier's response mode DSR activities would be covered by the provisions in this PAS regarding the operation of a DSRSP.*

4.5 ESA manufacturers

*COMMENTARY ON **4.5***

As an economic or environmentally friendly benefit, manufacturers can choose to develop and sell appliances that can flexibly manage their use, production or storage of electricity. The flexibility can be controlled by time, tariff or external instructions (e.g. called DSR).

Within this PAS, ESA is a defined term, which means the asset is compliant with PAS 1878:2021, and includes the associated CEM functionality.

The manufacturers are responsible for designing and supplying ESAs that can respond to routine mode and/or response mode DSR signals as specified in PAS 1878:2021. The manufacturers are responsible for any CEM providers operating on their behalf.

Depending on the type of ESA, the potential DSR functionality should include one or more of the following capabilities:

a) reducing demand;
b) deferring demand;
c) expediting demand;
d) increasing demand;
e) decreasing generation; or
f) increasing generation.

***NOTE 1** Some ESAs can detect and respond to changes in the frequency of the supplied electricity and may be used as a called frequency response service as set out in PAS 1878:2021, **5.5.5**.*

Manufacturers should not collaborate with DSRSPs in a manner which causes consumer lock-in or prevents interoperability of DSR services.

***NOTE 2** Manufacturers of PAS 1878:2021 compliant ESAs might innovate by providing additional functionality that can be accessed by DSRSPs or other energy management services, provided that such enhancements do not compromise the interoperability of the ESAs.*

Manufacturers should not hinder consumer engagement with DSRSPs and should enable DSRSP subscription.

4.6 National regulatory authority

Given the potential impact on grid stability of unauthorized or inappropriate DSR interventions, the national regulatory authority (NRA) in overseeing the operation of electricity markets may determine that only approved organisations should provide DSR services within their jurisdiction. Such approval, where required, may be undertaken by the NRA or by a registration organization appointed for the purpose. The NRA, or its regulated entities utilising DSRSP services, should, where required, set out what criteria a potential DSRSP should meet and maintain.

***NOTE** The criteria employed to assess the potential DSRSP can address a range of issues regarding the applicant's governance, capacity and capabilities, including its ability to address the recommendations set out in Clauses **6** to **10**.*

5 The four principles for consumer DSR

*COMMENTARY ON CLAUSE **5***

*The four principles for consumer DSR are set out in **0.5**. This Clause identifies high level service requirements that a DSRSP addresses when designing and operating a DSR service.*

5.1 Interoperability

A DSRSP should design and operate its service so that:

a) a consumer, or their authorized representative, can switch to a different DSRSP at any time without the need to purchase or install any new equipment, or the need for a premises visit from an installer or supplier of equipment;

b) it is supported by the definition in PAS 1878:2021 of the minimum required common data model, information model and communication protocol;

c) an ESA can work seamlessly across any appropriate DSR service operated by any DSRSP that the ESA is technically capable of meeting;

d) DSR signals are communicated to ESAs using the standards specified in PAS 1878:2021, which support interoperable commands and languages; and

e) it satisfies the performance and security requirements for the interface between the DSRSP and consumer premises as recommended in this PAS and specified in PAS1878:2021.

5.2 Data privacy

*COMMENTARY ON **5.2***

*See **4.3.7** regarding the role of third parties in handling consumers' data as part of a consumer relationship management service. For systems and services handling consumers' personal data, attention is drawn to the applicable data privacy legislation.*

A DSRSP should design and operate its service so that:

a) all communication in the DSR system includes authentication and encryption to prevent unauthorized access to or disclosure of consumer data;

b) personal data, when required, should be secured when transmitted between the consumer, or their authorized representative, and the DSRSP;

c) only the minimum amount of consumer data needed to operate a DSR service is shared with DSRSPs;

d) consumers, or their authorized representatives, are in control of any data exchanged with or collected by third parties arising from their use of a DSR service;

e) clear consent procedures are in place that enable consumers, or their authorized representatives, to make informed decisions regarding data sharing and to update their consent as appropriate;

f) personal data is only transferred between components of the DSR system if absolutely necessary and is limited as much as possible; and

g) personal data is not transferred to/from third parties without the knowledge and permission of the consumer, or their authorized representative.

***NOTE** In g) above the reference to third parties is to organizations other than those contracted to act on the DSRSP's behalf.*

Where a DSRSP shares data with third parties, it should maintain an auditable history of data sharing/access that is available to consumers on request.

5.3 Grid stability

A DSRSP should design and operate its service so that it:

a) reduces the risk that inappropriate operation of ESAs would result in supply outages of the electricity transmission and/or distribution networks;

***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.*

b) is able to determine whether each DSR event is subject to a randomized timing offset if it, or a regulated electricity market participant requesting the intervention, decides that such an offset is necessary for grid stability;

c) can detect and respond to anomalies concerning intervention messages sent to ESAs, in terms of the:
   1) number or rate of messages sent/received;
   2) type of messages sent/received; and
   3) content of message sent/received;

   NOTE 2 *The thresholds and criteria for anomaly detection may be set by the TSO or the national regulatory authority and depend on the nature and scale of the DSRSP's operations.*

d) can accommodate potential loss of communications between the DSRSP and an ESA;

e) maintains accurate and up-to-date knowledge of the flexibility available, based on the flexibility updates provided by ESAs that are subscribed to their service, thereby allowing timely iteration of call responses to achieve the required demand outcome; and

f) ensures that proper account is taken of any local (property-specific) constraints that might exist.

5.4 Cyber security

A DSRSP should design and operate its service so that it:

a) reduces the risk, to a level that is appropriate to the service, of compromise, interference or denial of communications between the DSRSP, its customers (TSO and DNO), and consumers and their subscribed ESAs;

   NOTE 1 *In addressing potential denial of communications, this relates to the DSRSP's communications interfaces and where applicable the communications interfaces of cloud-based CEMs. It is not intended to cover the individual consumer premises, although the DSRSP will be cognizant of the impact on its service arising from loss of connectivity due to communications/network outages affecting consumer premises on an ISP or geographic basis.*

b) reduces the risk of unauthorized access to, control or use of the DSRSP's system(s);

c) reduces the risk of unauthorized access to or control of an ESA;

   NOTE 2 *Provisions regarding the security of individual ESAs and their associated CEM are specified in PAS 1878:2021. DSRSPs will be expected to design their systems so as to prevent unauthorized access to and control of ESAs subscribed to their DSR service.*

d) applies the above recommendations regardless of the communications pathways chosen for implementation of DSR functionality; and

e) its system and services comply with applicable cyber security advice or guidance as issued by the national regulatory authority and/or national security authorities.

NOTE 3 *This PAS provides recommendations for the storage and exchange of information between the DSRSP and ESA, and for the authentication of the CEM, DSRSP, the ESA and the ESAG.*

6 Security principles

6.1 General

In the context of this PAS, data privacy (Clause **8**), electricity grid security (Clause **9**), and cyber security (Clause **10**) are essentially related security topics, which are the responsibility of, and should be taken into account by, the DSRSP when developing its security strategy. Security of the electricity grid is dependent on the cyber security of the DSR system, specifically preventing threat actors from creating situations which threaten the stability and operation of the grid through manipulation of electricity consumption and/or production across a large portfolio of ESAs.

***NOTE 1** Cyber security is dependent on the implementation of appropriate security across:*

a) the physical DSR architecture;

b) the operational processes followed by the DSRSP;

c) the personnel security of those operating the DSR service and those having access to consumers' personal data; and

d) the technological solutions used to deliver the DSR service and to affect the flow of communications across the end-to-end DSR system.

***NOTE 2** Data privacy depends on the adoption of appropriate and proportionate measures throughout the DSR service that address the security goals of confidentiality and control. Data integrity depends on both the processing of data by the DSRSP and the authenticity of data supplied by ESAs and/or users. For a general overview of cyber security principles in complex engineering systems, see PAS 1085:2018.*

***NOTE 3** In the context of this PAS, cyber security relates to both interactions by DSRSPs with third parties (e.g. the ESO, DNOs and EV chargepoint operators) and the potential impact of DSRSPs' communications with their portfolios of ESAs on the operation of the electricity supply network (i.e. transmission and distribution). Effective cyber security requires an integrated approach across the four security domains (i.e. people, physical, process and technical security), for example, to ensure that an insider does not exploit vulnerabilities in business processes to compromise the DSR service or maliciously use consumers' personal data.*

***NOTE 4** Annex A provides a mapping of selected standards and guidance that are relevant to the contents of Clauses **6**, **8** and **10**.*

6.2 Security governance

*COMMENTARY ON **6.2***

*As illustrated by the high-level trust models in Annex B, the operation of a DSR service involves a complex collection of trust relationships, including the majority of the actors listed in Clause **4** and elements of the end-to-end system. The choice of technical architecture will have a significant impact on these relationships, in particular the use of cloud-based CEM and ESAG acting as an intermediary between the DSRSP and the ESAs they control.*

6.2.1 Senior management understanding of security issues

*COMMENTARY ON **6.2.1***

*The concept of identifying information security requirements is identified in BS EN ISO/IEC 27000:2020, **4.5.2, 4.5.3** and **4.5.4**. The approach outlined below is adapted from the good practice in PAS 7040:2019, Clause **7** and in BS EN ISO 19650-5:2020, Clause **5**.*

The Board toolkit [6] prepared by the UK's National Cyber Security Centre (NCSC) and Passport to good security for senior executives [7] prepared by the Centre for the Protection of National Infrastructure (CPNI) provide guidance for senior management on cyber security and security issues respectively.

6.2.1.1 Situational awareness

The DSRSP's senior management should put in place policies, processes and procedures to research, document, demonstrate and maintain an understanding of the range of potential security issues that are applicable to its business, assets, personnel and the environments and ecosystems in which it delivers DSR services. This research should assess potential:

a) threat actors and their motivation;

b) vulnerabilities in the DSR system architecture and processes; and

c) impacts on the security domains and goals enumerated in **6.3.1** and **6.3.2** respectively.

When researching security issues the DSRSP should prioritize those affecting the safety, security and stability of the electricity transmission and distribution system, and the information security and assurance of industry and consumer information required to operate the DSR service.

6.2.1.2 Understanding the DSR ecosystem

In developing the understanding in accordance with **6.2.1.1**, the DSRSP should also assess and document the security and performance issues arising from the use of technologies and services outside their direct control, including:

a) the communications channels used to interact with the regulated electricity market participants and consumers' ESAs;

b) any intermediate services or functionality located between the DSRSP's system and the ESA in consumers' premises, e.g. connectivity to consumers' premises via a cloud-based CEM provided by a third party; and

__NOTE__ Communications channels with other parties might also be relevant to the security of DSR service provision, e.g. energy suppliers or information providers such as the Met Office.

c) the connectivity within consumers' premises to devices supporting the DSR service, e.g. broadband routers, individual ESAs and any CEM or ESAG.

6.2.1.3 Understanding the criticality of an asset or assets to DSRSP's operations

For each asset or aggregated group of assets the DSRSP should:

a) assess and identify its criticality and the impact of:
   1) its loss, corruption or compromise;
   2) its failure, either partially or as a whole;
   3) its misuse or abuse (whether unintentional or malicious); and
   4) its incorrect operation on ESAs and/or the exploitation of consumers;

b) identify and assess its vulnerabilities; and

c) identify and assess potential threats and opportunities.

6.2.1.4 Identifying and responding to security incidents

The DSRSP's senior management should be responsible for overseeing the handling of incidents and providing where applicable appropriate and timely reports to the relevant national authorities.

The DSRSP should put in place policies, processes and procedures for identifying and responding to security incidents affecting DSR operations and the protection of consumer information. These arrangements should be documented and address security risks inherent in processing consumer and DSR service data by third parties, with guidance provided to suppliers on the timely notification to the DSRSP of any relevant security issues within third parties' operations.

__NOTE 1__ NCSC has prepared guidance on the handling of cyber security incidents [8].

__NOTE 2__ Relevant security issues within third parties' operations will include those that have or might have affected consumer and/or DSR service data. It is good practice to report both security incidents and near misses.

6.2.2 Composition and integration risks

In its delivery of DSR services, the DSRSP should assess the security risks that arise through the composition and integration of components, sub-systems and systems, and, where appropriate, their interaction as systems-of-systems.

__NOTE__ Composition and integration risks arise from the selection of elements and how they are integrated. Complementary weaknesses in two or more elements that are being integrated might significantly increase the risks of exposure of the combined vulnerability and subsequent exploitation (see __10.4.3__ for further information of these risks on cyber security).

6.3 Holistic approach to security

COMMENTARY ON __6.3__

The concept of adopting a holistic approach to security is described in PAS 185, PAS 1085:2018 and PAS 7040:2019.

6.3.1 Security domains

From a security perspective, a holistic approach should be adopted, as illustrated in Figure 3, that addresses the eight security goals across the four security domains and is subject to appropriate governance:

a) **people**, i.e. all those that have access to the DSR system and the data/information it contains;

b) **physical**, i.e. the physical environment in which components of the DSR system are deployed, ranging from the devices installed in consumers' premises through to any remote (e.g. cloud-based) service provider;

c) **process**, i.e. the business processes used to deliver the DSR service, including any contractual or regulatory controls limiting the load that can be switched over a specific period; and

d) **technical**, i.e. addressing security issues arising from technology used in and design of the components of the end-to-end DSR system, including the data and/or information that is created, processed and stored in it.

NOTE 1 *The eight security goals in Figure 3 (confidentiality, availability, safety, resilience, possession, authenticity, utility and integrity) are applicable across the four security domains (people, physical, process and technical). For example, the physical composition of the DSR architecture can affect the integrity of the data and/or information it processes, which might result in a loss of availability of a safety critical process leading to potential harm to a consumer, EV or premises, or the failure of a DSR process.*

NOTE 2 *For the purposes of this task the safety aspects of DSR have not been addressed as they are part of a separate study.*

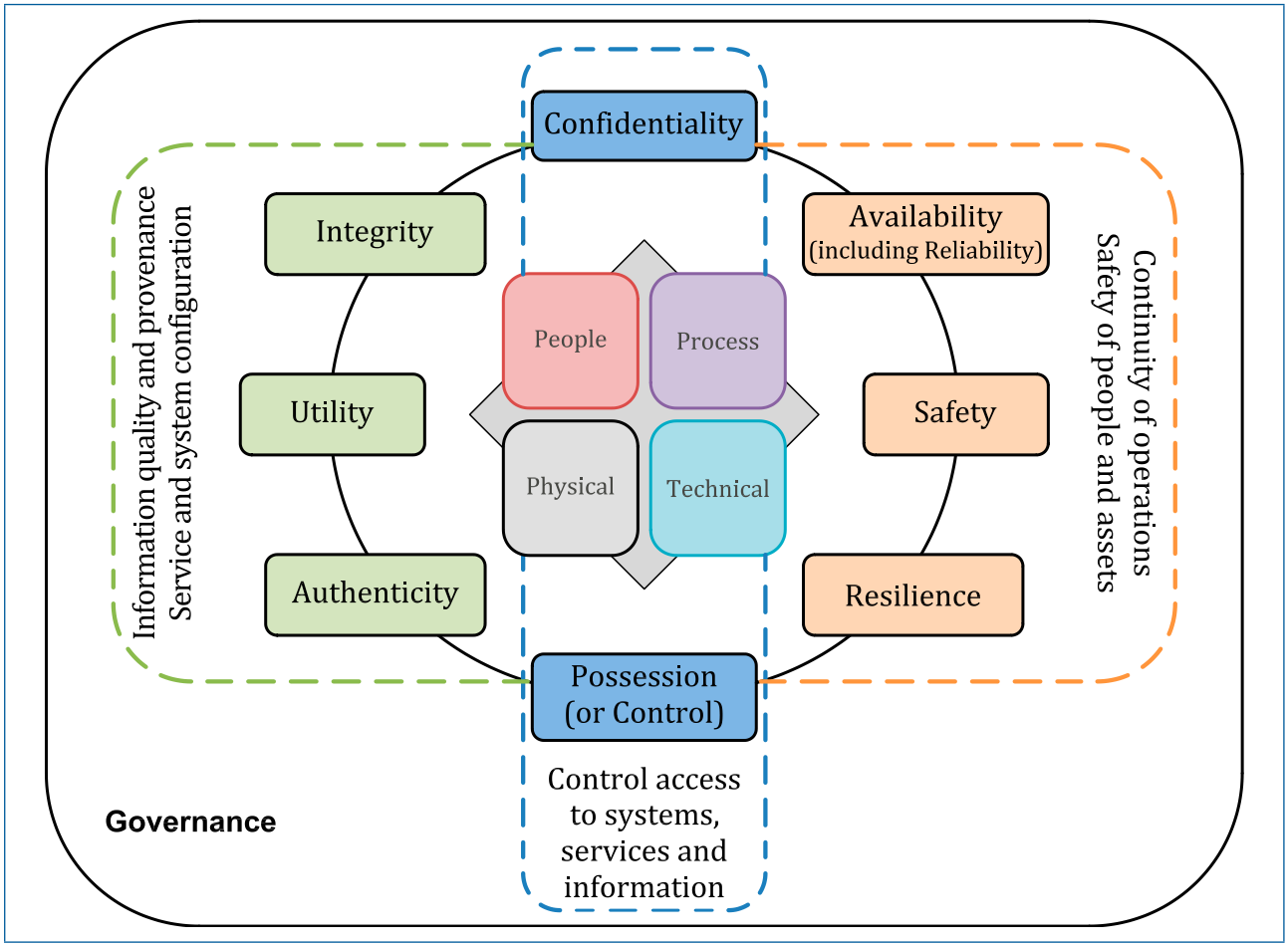
6.3.2 Security goals

When designing and implementing their technical, information and business architectures the DSRSP should apply the security goals identified in **6.3.2** to its DSR services, and to any supporting elements (e.g. CEMs, ESAs, etc.) and/or systems, through appropriate personnel, physical, process and/or technical security measures. In a DSR context the DSRSP should interpret the security goals as follows.

a) Confidentiality, i.e. the control of access, and prevention of unauthorized access to DSR systems, and sensitive data and information, in isolation or in aggregate.

b) Possession, i.e. DSR systems and associated processes or services should be designed, implemented, operated and maintained so as to prevent unauthorized control, manipulation or interference, and so that data and/or information are only used in accordance with the DSRSP's obligations, licence or contractual rights.

Figure 3 – Security domains and goals



c) Availability (including reliability), i.e. the data, information, DSR systems and associated processes should be consistently discoverable, accessible, usable and, where appropriate, can be disclosed in an appropriate and timely fashion.

d) Safety, i.e. DSR systems and related processes should be designed, implemented, operated and maintained so as to prevent the creation of harmful states, which might lead to injury or loss of life, or unintentional environmental damage, or damage to assets.

e) Resilience, i.e. the ability of data, information, DSR systems and any associated processes or services to transform, renew and recover in a timely way in response to adverse events.

f) Integrity, i.e. maintaining the completeness, accuracy, consistency, coherence and configuration of data, information and DSR systems.

NOTE 1 *When considering the integrity of communications between the DSRSP and an ESA, this includes the non-repudiation of data flowing in either direction.*

g) Utility, i.e. data, information and DSR systems should remain usable and useful across the life cycle of the data and information, and of any associated asset, individual, organization, DSR system and connected ESAs.

h) Authenticity, i.e. data and/or information input to and output from DSR systems, the state of the systems and any associated processes, data and/or information should be verified and certified as genuine.

The DSRSP's overall security governance regime should establish appropriate accountability regarding the actions and behaviour of its personnel and supply chain.

NOTE 2 *Harmful states affecting the electricity transmission and distribution system include:*

a) rapid modulation of aggregated loads which have sufficient magnitude to disturb the quality or stability of supply within the transmission network; and

b) switching loads within the distribution network so as to cause instability in parts of the network due to uneven spread of the modulated premises.

NOTE 3 *The security goals are applicable to systems both as supplied and operated by the DSRSP and any ESA-related components, including the CEM.*

7 Interoperability

*COMMENTARY ON CLAUSE **7***

*See **4.3.10** regarding third parties contracted to act on behalf of DSRSPs.*

7.1 Purpose of this principle

This principle aims to maintain consumer choice, so that the consumer has freedom to change service providers and avoid lock-in due to use of proprietary protocols or system interfaces. A DSRSP should offer a service that delivers the capability for an ESA to work seamlessly across any appropriate DSR service operated by any DSRSP.

***NOTE** In jurisdictions where the national regulatory authority requires DSRSPs to be approved, such approval may include demonstrating the provision of an interoperable DSR service.*

7.2 Practices to be adopted for provision of consumer DSR services

7.2.1 Prevention of vendor lock-in

DSRSPs and ESA manufacturers should design ESAs and DSR services, and in the case of DSRSPs operate services, so as to avoid vendor lock-in, for example through the use of proprietary protocols or system interfaces. This should include adoption of measures to:

a) enable consumers to subscribe any ESA that is normally available for purchase within the jurisdiction in which the consumer's premises are located (subject to the DSRSP's business model supporting use of that asset type of ESA);

   ***NOTE 1** The DSRSP will be aware that consumers are likely to have ESAs from more than one manufacturer so that their service design can accommodate the safe and secure handling of interactions between the CEM and the ESAs.*

b) enable consistent interface between any CEM and the DSRSP in its design and operation with the requirements specified in PAS 1878:2021; and

c) verify that the services operated by the DSRSP do not disrupt or deny access to other services delivered to the consumer's premises.

   ***NOTE 2** The phrase "disrupt and deny access" does not apply to authorized interventions in respect of an ESA that has been subscribed to a DSR service.*

Where the DSRSP communicates with the CEM and/or ESAs via the internet, the DSRSP's service should not interfere with or prevent the use of other internet-based services or usage through the same broadband connection.

7.2.2 Ease of DSR service transfer

The DSRSP should design and deliver DSR that minimizes barriers should a consumer wish to change DSRSP. Where a DSRSP is notified by a consumer, or their authorized representative, that they wish to unsubscribe the DSR service, the DSRSP should without delay stop using the the ESA(s) as part of its portfolio, as specified in PAS 1878:2021.

Where the ESA was subscribed as part of a third-party portfolio, and if the notification to unsubscribe is received by the DSRSP via the ESA-to-DSRSP interface, the DSRSP should notify the third party of the unsubscribe request.

7.3 Practices to be adopted for compliance with PAS 1878:2021

The DSRSP should design and operate systems and services in line with requirements in PAS 1878:2021, including by using its Interface A specification.

8 Data privacy

*COMMENTARY ON CLAUSE **8***

*As illustrated in Figure 1 and Figure 2 and outlined in **4.3.7**, the DSRSP may have a contractual relationship with a third-party asset operator or manager who enrolls consumers into the DSR service. In these situations, consumers' personal data may predominantly be processed by the third party. However, it is likely that the DSRSP will process some personal data; for example, the address of a premises at which a subscribed ESA is located or the meter reference for that property. The responsibilities outlined in this clause are applicable to all parties processing personal data, with shared responsibilities occurring where one party is sharing with another personal data that has been collected from consumers.*

The secure transmission and storing of personal data by any controlling party is covered by data protection legislation. Existing practices for industrial DSR are only partially relevant to data privacy; the key difference is the legislation covering protection and use of consumers' personal data. In the case of industrial DSR, the issue primarily relates to commercial confidentiality rather than data protection. Privacy legislation generally applies only to individuals and not to information about industrial or commercial entities and their business activities.

In the UK privacy requirements largely stem from the provisions of the Data Protection Act 2018 [4], which encompasses the provisions of the GDPR [5] and their application in UK law. This Clause identifies some of the practical issues associated with addressing these requirements in a DSR context.

8.1 Practices to be adopted for provision of consumer DSR services

8.1.1 Identification and protection of personal data

In respect of any personal data processing by a DSR system, the DSRSP should identify, document, demonstrate and mantain an understanding of the risks:

a) to the data or information;

b) arising from associations and behaviours that might result in disclosure, or lead to unintended release of information, about the pattern-of-life of individuals or groups of individuals and/or pattern-of-use of the premises and/or connected ESAs;

c) arising from data and/or information aggregation:

   1) within the organization; and

   2) through the data and/or information generated and/or processed by its products and/or systems, and any related services.

In assessing the pattern-of-life issues, the DSRSP should make consumers aware of the collection and proposed use of such data and the potential consequences were it to be misused by a third party. Consumers should be given the right to opt out of sharing of pattern-of-life data, at both premises and ESA levels, by the DSRSP with any third party.

8.1.2 Processing of personal data

Where a DSR system processes or stores personal data, the DSRSP should determine the measures and/or actions required so that the risks identified in **8.1.1** can be minimized, mitigated or managed in a timely manner. The DSRSP should produce and maintain documentation and evidence to demonstrate that the design complies with the following recommendations.

a) The processing of personal data should be minimized.

b) Processes should be in place to allow data subjects to:

   1) establish what personal data is held by the organization;

   2) ascertain for what purpose it is being held;

   3) understand the lawful basis for its process;

   4) opt in/out of processing as appropriate; and

   5) exercise the data subject's right to be forgotten.

   ***NOTE 1** See **8.1.4** regarding changes of premises and ESA user.*

c) Personal data should be stored for the shortest practicable period.

d) A data retirement plan should be put in place for the secure destruction of all personal data when it is no longer required.

e) Wherever practicable the design should reduce privacy risks through use of privacy enhancing technologies.

f) Any personal data stored within the DSR system and connected ESAs should be afforded enhanced technical and physical protection to prevent unauthorized access by personnel servicing or maintaining ESAs.

g) Any personal data stored outside the DSR system and connected ESAs should be afforded protection commensurate with its sensitivity and good industry practice.

NOTE 2 *Attention is drawn to the relevant prevailing data protection legislation of the jurisdiction in which the ESA is located or in the case of EVs is registered and normally used.*

8.1.3 Security of consumer enrolment website or smartphone application

Where a DSRSP, or a third party enrolling consumers on behalf of the DSRSP, uses a website or application to enrol consumers and manage their subscriptions, the website and/or application should be designed to be secure-by-design, with encryption implemented to protect data-at-rest and data-in-transit.

NOTE *Where a CEM is used to process consumer data as part of the enrolment process or management of the consumer's subscription, the security provisions in PAS 1878:2021 apply to the protection of personal data.*

8.1.4 Storage of personal data

Where a DSR system stores personal data, the DSRSP should design a system that allows a consumer to exercise their right to be forgotten by permanently deleting their personal data from the DSR system(s).

So as to prevent the unintentional sharing of a consumer's pattern-of-life and/or the pattern-of-use of an ESA, a DSRSP should address a consumer's right-to-be forgotten where:

a) a consumer changes premises and a subscribed ESA remains at their old premises; or

b) there is a change of premises of a subscribed ESA;

NOTE *For example, a consumer might sell or transfer an ESA to another consumer, and unless the original consumer unsubscribed the ESA there is a risk that personal information associated with the ESA could be disclosed to the new consumer.*

8.2 ESA manufacturer

Where an ESA manufacturer collects and processes consumer personal data it should address the requirements set out in PAS 1878:2021.

8.3 Data and information sharing agreement (DISA)

COMMENTARY ON ***8.3***

The concept of data-sharing agreements is in use across a number of industries and sectors and relates to establishing a clear enforceable agreement between the parties sharing data. The approach set out in this Clause is based on PAS 185 and PAS 1085:2018, which describe data sharing agreements in a smart city context. By placing the data-sharing agreements in a standalone document, the parties involved are able to disclose the arrangments to consumers, regulators and other interested stakeholders, without needing to reveal any wider commercial relationships.

8.3.1 Development of a data sharing policy

The DSRSP should develop, implement and periodically review an overarching policy regarding the sharing of data and/or information, taking into account the corporate risk appetite and providing an aggregated view of the acceptable level of sharing. The DSRSP should publish the policy on its website to inform consumers what information it shares, or intends to share, for what purposes and with whom.

NOTE *This policy is to be used to inform the development, acceptability, application and termination or retirement of individual DISAs.*

8.3.2 Establishing a DISA prior to sharing data and/or information

Where a DSRSP shares or intends to share consumers' personal data with a third party, the sharing arrangements should be agreed by the parties involved and documented in a DISA.

The DSRSP should put in place this agreement, known generally as a DISA, prior to sharing any sensitive or potentially sensitive data or information that could be used to cause harm to:

a) the electricity distribution system;

b) DSR systems-related assets;

c) the services it delivers, the premises where it delivers DSR services and their use or occupants; and

d) the ESAs with which it communicates.

With the exception of DISAs related to national security and/or the protection of national infrastructure, the DSRSP should publish all DISAs it enters into on its website.

NOTE 1 *The aim of the DISA is for the party providing the data and/or information to put in place appropriate and proportionate controls on its use by the recipient; this is intended to have legal effect (i.e. the parties involved can seek legal remedies in the event of a breach of the agreement). The existence of data sharing agreement(s) may be publicised by the DSRSP in any privacy or data protection policies it publishes.*

Before any data and/or information is made widely available, the DSRSP should verify that the disclosure does not include sensitive or potentially sensitive data or information, both in isolation and in aggregate.

NOTE 2 *Once data and/or information has been published on the internet, or otherwise made publicly available, it is virtually impossible to delete, destroy, remove or secure all copies of the released data and information. In addition, the release of aggregated, apparently innocuous data and information, can result in exposure of sensitive or security information.*

8.3.3 Situations requiring a DISA

The provisions of **8.3.2** should apply to all situations where:

a) the DSRSP, or a third party in a contractual relationship with the DSRSP, is designing, implementing or operating systems or services that process data or information relating to:
   1) ESAs and their use, location or ownership; or
   2) consumers and occupants of premises where ESAs are managed by its DSR services; or

b) where this data or information is shared with or processed by a third party, either:
   1) in the DSRSP's supply chain; or
   2) as part of a service provided by the DSRSP to regulated electricity market participants.

NOTE *The term "process data" is interpreted as encompassing the various aspects of data processing covered by the Data Protection Act 2018 [4] and the GDPR [5], (i.e. the creation or collection, processing, storage, retrieval and deletion of data or information).*

8.3.4 Contents of a DISA

A DISA should detail, as a minimum:

a) the purpose, or purposes, of the sharing;

b) the potential recipients, or types of recipient, and the circumstances in which they might access or use the data and/or information;

c) the type of data and/or information to be shared;

d) the monitoring and auditing of the implementation of the sharing agreement;

e) the quality of the data and/or information to be shared, in particular its authenticity, coverage, accuracy, relevance and usability;

f) the requirements in relation to:
   1) where relevant, data protection and consumers' rights to opt in/out of data processing which is not related to the delivery of the DSR service. Unless an alternative lawful basis for processing can be identified, a consumer should be given the option to "opt out" of the processing (there is a requirement to "opt in" if the purpose of the DISA is for marketing purposes);

      NOTE 1 *For guidance on the lawful basis for data processing see the Information Commisioner's Office (ICO) website*[4]*.*

   2) permitted and prohibited rights of use of the data;
   3) obligations to notify the data owner and/or data controller in the event of a security incident, or any complaints regarding the quality of the data or information. The obligations should reference the relevant security incident management policies, processes and procedures as set out by the DSRSP.

      NOTE 2 *Given the international nature of ESA manufacturing, particular attention is drawn to the handling of data and information arising from variations in legal and/or regulatory requirements in different jurisdictions. This might be a significant issue where manufacturers offer consumers smartphone applications and/or cloud-based services to manage the operation of their ESAs. In these instances, the data and information might be stored in locations outside the UK, where there are limitations on the protection afforded to personal information.*

[4] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

g) data and/or information maintenance, including responding to notification of requests for erasure or correction, and the right to be forgotten;

h) data and information security, including the handling of security incidents and investigations undertaken by data protection authorities;

i) the arrangements for retention and/or purging of shared data and/or information;

j) procedures dealing with data subjects' rights, including access requests, queries and complaints; and

k) sanctions for failure to comply with the agreement and/or a security incident(s) caused by an individual member of staff.

8.3.5 Remedies for breach of DISA provisions

In the event of a security incident, or if there is evidence that data or information is not being managed and handled in accordance with the DISA, the DSRSP should have the authority to:

a) suspend the sharing agreement until the event or concerns have been investigated and any remedial measures have been agreed and implemented; or

b) terminate the sharing agreement and require purging or secure deletion of the shared data and/or information if the matter cannot be satisfactorily remedied.

NOTE 1 *Depending on the terms of the agreement, suspension might limit or prevent:*

a) further sharing of new data or information; and/or

b) use of existing shared data or information.

NOTE 2 *Depending on the nature of the breach there might be specific reporting requirements. Where such requirements exist the DISA may address the responsibilities of the parties involved to provide the necessary reporting in a timely manner.*

8.3.6 Periodic review of DISA

The DISA should be periodically reviewed, with the findings assessed by senior management, to establish the effectiveness of the sharing and to confirm that:

a) the data and/or information shared is precisely what was agreed, i.e. no additional data and/or information (e.g. additional attributes) has accidentally been made available;

b) there is still a legitimate purpose for the continued sharing of data and/or information;

c) the recipients of the data and/or information still need access to it, and where they do not, that access has been withdrawn;

d) the data and information quality and maintenance are to the agreed standards; and

e) the data security arrangements remain appropriate and proportionate, and that any complaints have been satisfactorily resolved.

9 Grid stability

*COMMENTARY ON CLAUSE **9***

The stability and security of the electricity grid is dependent on the trustworthy and secure operation of both individual organizations and the electricity supply chain as a whole. Given the paramount importance of reliable electricity supply to the safety, security and economic wellbeing of developed nations, governments and regulatory authorities typically require electricity supply chain organizations to meet specific governance, financial standing and operational security requirements.

The voltage and frequency stability of the public electricity supply is critical to the operational of national infrastructure and to the day-to-day activities of industrial, commercial and domestic end users. The TSO is responsible for balancing supply and demand across the transmission network so as to maintain grid stability and employs a range of flexibility options (i.e. reducing demand and/or increasing supply) to achieve this aim.

The electricity market and access to the transmission and distribution networks is governed by regulation and supporting market codes. These codes specify the business practices and rules both in terms of trading activities and codes of connection.

A number of the market participants are treated as supporting the critical national infrastructure and where their action or inaction might affect grid stability, they are subject to specific security requirements, both national and international, i.e. the Network and Information Systems Regulations 2018 [9]. Given the aggregate demand or generation that a DSRSP might effectively control and the potential for misuse of such control to affect grid stability, there is a need for DSRSPs to be subject to similar security requirements.

9.1 Approval of DSRSPs

Before an organization can commence operations as a DSRSP, a national regulatory authority may require that it should be subject to assurance requirements (see **4.3.2**). Where approval is necessary the requirements should take into account the grid stability principles set out in **5.3** and assess the DSRSP's ability and capability to satisfy them.

9.2 Organizations permitted to request response mode DSR interventions

Organizations permitted to request response mode DSR interventions are regulated electricity market participants, but this might vary from time-to-time. The national regulatory authority or the national market codes should specify how a DSRSP identifies those organizations that are permitted to request response mode DSR interventions.

In jurisdictions where DSRSP approval to operate response mode DSR services is required, regulated electricity market participants that are permitted to request DSR interventions should only make such requests to an approved DSRSP.

9.3 Authentication of response mode DSR service requests

A DSRSP should only process service requests on behalf of regulated electricity market participants. The authenticity and integrity of all such service requests should be validated.

9.4 Authorization to undertake response mode DSR service interventions

A DSRSP should not undertake response mode DSR interventions unless authorized to do so by a regulated electricity market participant, except for the purposes of testing. Where such testing involves sufficient load or generation to affect network stability, the DSRSP should inform the relevant DSO, and if appropriate the TSO.

9.5 Monitoring of response mode DSR service interventions

A DSRSP should monitor the message traffic to its portfolio of ESAs to verify that the rate, volume and nature of intervention requests is commensurate with the requested response-mode DSR services traffic.

Where a DSRSP detects inconsistencies or anomalies arising from this monitoring, it should investigate the cause and implement appropriate actions so as to maintain grid stability. If the cause is, or could be, related to a security incident, this should be reported in a timely manner to the relevant national authorities.

9.6 Monitoring and maintaining ESA portfolio status

A DSRSP should maintain:

a) up-to-date information on flexibility options from its portfolio of ESAs; and

b) awareness of active ESAs and inactive ESAs in its portfolio and only request DSR interventions from active ESAs.

10 Cyber security

*COMMENTARY ON CLAUSE **10***

The electricity industry is a target for malicious actors seeking to disrupt the electricity generation and supply, which can have significant economic and societal impact. To address the risks associated with the activities of these malicious actors, national authorities require organizations involved in the generation, transmission, distribution and supply of electricity to implement cyber security measures.

Organizations involved in the generation, transmission, distribution and supply of electricity are subject to a variety of cyber security requirements and recommendations, including:

a) legislation/regulation;

b) national guidance; and

c) industry specific guidance.

Security standards relevant to the design and operation of automation and control systems include IEC 62443-2-1 and IEC TS 62443-1-1.

The contents of this Clause are applicable to response mode DSR services involving consumer ESAs. The security of routine mode DSR services delivered by smart metering systems is addressed in the specifications for those systems.

10.1 Cyber security practices to be adopted for the provision of consumer response mode DSR services

*COMMENTARY ON **10.1***

A key feature of consumer response mode DSR is the nature of the ecosystem. It is a distributed control system comprising a system-of-systems, with potentially hundreds of thousands or millions of endpoints (ESAs) under the control of a DSRSP. ESA power profile information and DSR intervention commands flow through a diverse network owned and operated by numerous organizations. The aggregate effect of the DSR intervention commands are critical from a grid stability perspective as incorrect or unauthorized instructions could affect the operation of the transmission and/or distribution networks.

To address the cyber security of the consumer DSR ecosystem, a portfolio of security measures should be implemented, covering physical, personnel, process and technology aspects of the system-of-systems. The DSRSP approach to cyber security should conform to:

a) ETSI EN 303 645;

b) IEC 62443-2-1; and

c) IEC TS 62443-1-1.

The DSRSP should consider separation of networks used for operational and general IT systems as specified in IEC TS 62443-1-1.

In addition to meaures set out in the above standards, the DSRP's approach should address those measures covered in **10.2**, **10.3**, **10.4**, **10.5**, **10.6** and **10.7**.

10.2 Personnel security

*COMMENTARY ON **10.2***

The human element is often the weakest link in any business and can undermine technical and process security measures through careless or ill-informed actions.

10.2.1 Security awareness training

The DSRSP should maintain a culture of cyber security within the organization such that all personnel are made aware of misinformation, cyber security risks and security controls.

The DSRSP should provide general security awareness training to all personnel, which as a minimum should address the following topics:

a) cyber hygiene;

   ***NOTE** NCSC has published guidance on security training for personnel [10] and phishing [11].*

b) protection of data and information, including policies and procedures relating to sharing with third parties or publication of data or information about DSR-related systems; and

c) the DSRSP's policies and procedures regarding the security of its information, communications and operational technologies.

10.2.2 Identification of high-risk roles

The DSRSP should identity high-risk roles in the operation and lifecycle of its systems and services and any additional security training that might be required by personnel occupying these roles.

10.2.3 Management of personnel handling sensitive information or in high-risk roles

The DSRSP should establish that personnel handling sensitive information or occupying high-risk roles:

a) are subject to security screening and minimum competence requirements;
b) maintain records demonstrating that appropriate security awareness training has been undertaken;
c) are aware of their security responsibilities;
d) are accountable for their security-related behaviour; and
e) are in receipt of any additional briefing or training so that they can fulfil their role in a security-minded manner.

For those personnel within the DSRSP's organization and its supply chain who handle sensitive information or are in high-risk roles, the DSRSP should require that they undergo enhanced screening or vetting.

10.3 Supply chain security management

10.3.1 Understanding the supply chain scope, nature and risk

The DSRSP should research, document and manage security risks arising from its supply chain, including sub-contractors and service providers, by employing documented and auditable design, specification and procurement practices. When reviewing its supply chain, the DSRSP should assess the impact a cyber security incident affecting an external supplier could have on its operation, on DSR system-related assets and ESA, and any associated DSR services. This research should include:

a) identification of all external suppliers of assets and any related services employed in the delivery of DSR services;
b) identification of external suppliers proceeding beyond the first tier that are in contract with the DSRSP;
c) the DSRSP identifying the risks to the DSR service that might arise from modifications to the CEM or to the ESA performance and behaviour, whether authorized or not, and the impact of changes within or to the network and communications environment within which the ESAs operate; and
d) a cyber security maturity review of the external suppliers identified in a) above. The maturity review should be conducted using a recognized methodology, model or approach.

NOTE *Managing a complex supply chain and its inherent risks is challenging, as there is a loss of visibility and understanding as one moves further away from the purchaser through layers of contracts/sub-contracts. Further guidance regarding risk management in supply chains can be found in NIST SP 800-161 [12] and NCSC's Supply chain security guidance [13].*

10.3.2 Implementing and cascading security controls

The DSRSP should define and implement appropriate and proportionate contractual and operational measures required for the adoption of a security-minded approach throughout its supply chain. In fulfilling this requirement, the DSRSP should:

a) identify and agree with its suppliers how security risks are to be managed;
b) manage access to sensitive information and systems on a need-to-know basis, so that security measures can be maintained at an appropriate and proportionate level; and
c) require personnel within its supply chain who handle sensitive information to:
    1) be subject to security screening and minimum competence requirements;
    2) maintain records demonstrating that appropriate security awareness training has been undertaken; and
    3) undergo enhanced screening or vetting for those in high-risk roles.

10.4 Monitoring changes to threat landscape and emerging vulnerabilities

10.4.1 Situational awareness

The DSRSP should maintain situational awareness by monitoring:

a) cyber security risks and opportunities;
b) emerging cyber security threats and vulnerabilities; and
c) the organization's scope and security context.

10.4.2 Cyber threat landscape

The DSRSP should proactively monitor the threat landscape, taking into account known and emergent (i.e. unknown and/or potential) security risks, vulnerabilities and threat actors through collaboration and engagement with third parties.

***NOTE** The NCSC has set up a Cyber Information Sharing Partnership[5] (CiSP) to facilitate sharing of information between industrial organizations, both within and between sectors.*

10.4.3 Cascading and combinational effects of cyber security risks

The DSRSP should assess the cascading and/or combinational effects of cyber security risks arising both from human and natural causes that might affect its delivery of DSR services. Cyber security risks should not be considered in isolation; in a complex environment, such as delivery of DSR interventions, there might be considerable interaction between risks.

***NOTE 1** Combinational effects occur where there is a linear path of negative events. In the context of a cyber incident caused by a threat actor this is often called an "attack path", where a combination of vulnerabilities or security breaches allows the hostile party to significantly increase the impact of the attack. Combinational effects might also arise from a natural event coupled with a cyber incident.*

***NOTE 2** An example of a situation where composition and integration risks might occur is the use of a cloud-based CEM (i.e. a situation where the DSRSP is managing demand through a service provided by a third party).*

The DSRSP should maintain the end-to-end security of the DSR interventions (i.e. from its system through to consumers' premises). In this scenario, the communications links from DSRSP to CEM and CEM to ESA should be secured, and the trustworthiness and security of the CEM processing also requires a level of assurance to avoid man-in-the-middle type attacks. A similar approach should be adopted for use of in-home CEMs and any other architectures that deliver a PAS 1878:2021 compliant DSR service.

***NOTE 3** Cascading effects occur where there is a non-linear path of events occurring, including amplification and subsidiary negative events or outcomes. The cascade effect is particularly likely to occur in complex systems, i.e. systems-of-systems, where there is not a simple linear relationship between systems or sub-systems. In these cases, rather than the effect of the risk spreading in a simple longitudinal fashion, the effect spreads like a ripple affecting multiple assets that might not be directly connected to each other.*

10.4.4 Cyber security monitoring of DSRSP systems

The DSRSP should proactively monitor the systems used to deliver its DSR service so as to identify potential security breaches and facilitate a timely mitigation response. The monitoring should address existing and emerging threats as identified through situational awareness (see **10.4.1**) and its knowledge of the threat landscape (see **10.4.2**).

The security monitoring should include the DSR's internal systems and the connectivity as far as the Energy Gateway at consumers' premises.

***NOTE** Where CEM functionality is delivered outside of consumers' premises, the DSRSP needs timely reporting from the third party delivering the CEM functionality that there is no identifiable interference with and/or compromise of the connection between the CEM and the ESA.*

Where a DSRSP detects a security breach, becomes aware of a potential incident, or a near miss occurs, the incident or event should be handled in accordance with the DSRSP's incident management policy (see **6.2.1.4**).

10.5 Communications, data and information security

10.5.1 Protection and control of data and information

10.5.1.1

The DSRSP should develop, record, implement and manage appropriate and proportionate policies, processes and procedures relating to security-minded communications, data and information management. These should be based on an understanding of the security implications associated with the loss, compromise, unauthorized manipulation or change of data and/or information, as determined in **6.2**.

10.5.1.2

The DSRSP should secure and control the storage, transmission and processing of data and information.

The protection and control of data and information encompasses more than simply encrypting communications links between the DSRSP and third parties. The data and information should be protected so that it is not possible for an unauthorized individual, system or process to access, modify or delete data and information:

a) at rest, i.e. data stored by systems used to deliver DSR services;

[5] Available at: https://www.ncsc.gov.uk/section/keep-up-to-date/cisp.

b) in transit, i.e. when data is being transferred between systems, both within the DSRSP organization and in its interactions with third parties (e.g. consumers, DNO and TSO); and

c) in use, i.e. when data is being processed by DSR systems.

10.5.2 Communications security

10.5.2.1

Whilst the interfaces between the DSRSP and the TSO, DNO and, where applicable, suppliers, are outside the scope of this PAS, they should be secured. As a general principle, if a DSR system connects to an external interface operated by the TSO, DNO or an electricity supplier, the DSRSP should design connections and exchange of data and/or information so that the identity and trustworthiness of the third party's end-users and/or systems can be established using appropriate secure authentication schemes and the communications channel secured throughout the exchange of messages.

10.5.2.2

The interface used by the DSRSP to distribute DSR service messages and to receive service responses and information from CEMs and ESAs or any other system should protect the confidentiality, integrity and authenticity of message content.

10.5.2.3

The protection required in **10.5.2.2** should be implemented using a transport layer security (TLS) or internet protocol security (IPsec) as follows.

a) The digital certificate used by the DSRSP should be signed by a trusted certificate organization.

b) For connections to CEMs over interface A, TLS (Version 1.3 or above) should be used and communications should be configured to use the cipher suites and certificate sizes recommended by PAS 1878:2021, **6.8**, or the national regulatory authority, or other competent national authority, and not be allowed to downgrade security on handshake.

NOTE 1 *In the UK, the NCSC has published TLS guidance [14].*

c) For connections between a DSRSP and any sub-contracted third party, including cloud based communications, the following should be used:

1) an IPsec or TLS virtual private network (VPN) gateway, which can be configured to support a strong cryptographic profile; or

2) a TLS (Version 1.3 or above) secured API.

NOTE 2 *In the UK, TLS guidance [14] and NCSC advice on IPsec [15] may be used to ascertain whether the gateway supports a good profile.*

10.5.2.4

*COMMENTARY ON **10.5.2.4***

A digital certificate ceases to be valid if it is tampered with, cancelled by the issuing authority or it expires.

The DSRSP should design its systems so that messages are not sent to CEMs in the event that the DSRSP's digital certificate is no longer valid. DSRSPs should:

a) check the validity of the CEM/ESA certificate; and

b) not process messages where the CEM/ESA digital certificate has expired or is no longer valid.

CEMs should:

1) check the validity of the DSRSP's certificate; and

2) not process messages where the DSRSP's digital certificate has expired or is no longer valid.

10.5.3 Security documentation

10.5.3.1

To evidence compliance with the recommendations in **10.5.1**, when designing or modifying a DSR system or a DSR system-related asset, and any related service(s), the DSRSP should assess and document the following aspects:

a) the data and/or information that needs to be processed by the DSR system or DSR service-related asset and the lawful basis for its processing;

b) whether the data and/or information:

1) should be stored by the DSR system or DSR service-related asset and if so for how long;

2) can be deleted by an authorized person; and

3) is shared with other DSR systems or DSR service-related assets, and if so identify which assets and/or system(s) and the rationale for sharing it;

c) the value and sensitivity of the data and/or information;

d) the potential for personal data to be extracted from data sets or sets of messages; and

e) the potential need for protection of data, at rest, in transit and when in use (see **10.5.4**).

10.5.3.2

The documentation produced in accordance with **10.5.3.1** should be maintained under configuration control and updated as necessary to reflect developments in the design and integration of the DSR services over their lifecycle and the ESAs to which the services are connected.

10.5.4 Protection of data and information in DSR systems

Taking into account the analysis specified in **10.5.1** and **10.5.3.1**, the DSRSP should design DSR systems so that data and information are protected and appropriately secured:

a) in transit, i.e. when being transferred between different DSR services and any related products and/or systems, including the wider electricity supply, transmission and distribution system;

b) in use, i.e. during processing or display; and

c) at rest, i.e. when stored in a DSR system, including information stored in ESAs.

10.5.5 Forensic readiness of DSR systems

The DSRSP should verify that the design and implementation of the software, systems and services it delivers support the forensic recovery of data and information following any safety or security related incident.

NOTE *The provision of system logs, including security-related logging, is a key element in the design of forensically ready systems. PAS 1878:2021 includes the provision for ESA to log security-related activity. A DSRSP might need to retrieve such logs as part of an investigatin into a security incident (see also* ***6.2.1.4*** *regarding incident handling).*

10.6 Security of CEM and ESA components employed in delivery of DSRSP's services

10.6.1

The DSRSP should treat CEMs and ESAs that it interacts with to deliver DSR interventions as part of its supply chain.

10.6.2

The DSRSP should implement appropriate and proportionate technical measures to assure the correct operation of the CEMs and ESAs it interacts with. This assurance should comprise a combination of the following:

a) validation and verification of the current configuration of any software/firmware/reference data employed by the CEMs and ESAs. These checks should be applied upon sign-up by a consumer or third-party of an ESA with a DSRSP. The checks or tests performed should assure that the ESA and any associated CEM:

   1) is running the latest build of software/firmware;

   2) has not been tampered with (e.g. subject to an unauthorized modification); and

   3) is using the correct version of any reference data.

   Only when the validation and verification has been successfully completed should the DSRSP accept the ESA/CEM combination into service;

   NOTE *The nature of the checks are determined by the design of the ESA and/or CEM and might for example involve checking a cryptographic code signature applied by the manufacturer.*

b) periodic checking, detection, logging and reporting of incorrect, out-of-date, or otherwise compromised or potentially vulnerable or insecure configurations;

c) the frequency of checks on individual ESAs and CEMs should be risk-based and proportionate to the nature of the ESA and its load under control, and

d) daily or more frequent checks (where required) where the aggregate load under control by the CEM (e.g. for cloud-based CEMs) is orders of magnitude larger than the load controlled by a CEM in a consumer premises.

Where there are or might be concerns about the correct operation of a CEM or ESA, the DSRSP should remove affected elements from the available portfolio of controlled appliances and notify the registered contacts for the affected elements.

10.7 Secure-by-design

10.7.1 Evidencing the DSR system is secure-by-design

The DSRSP should establish, document and operate policies, processes and procedures such that all new designs are conceived and implemented using a product and/or service lifecycle that embraces secure-by-design.

NOTE 1 *The UK government has published a report advocating a fundamental shift in approach; moving the burden away from consumers having to secure their devices or products and instead ensuring that strong security is built in. The Secure-by-design report [16] advocates a fundamental shift in approach to securing IoT devices and related services, by moving the burden away from consumers and ensuring that security is built into products by design. For example, the use of hard coded or default passwords in devices is discouraged.*

NOTE 2 *PAS 1878:2021 addresses the secure-by-design aspects of ESAs and CEMs.*

10.7.2 Addressing common vulnerabilities

A DSRSP should design, operate and maintain its processes and systems so as to:

a) address known security vulnerabilities in the architecture, processes and technology (hardware and software) employed;

b) minimize the risk that unauthorized individuals (internal or external) could initiate, modify or terminate a DSR intervention; and

c) minimize the risk of incorrect translation of a service request into service messages sent to subscribed ESAs.

Assessing known risks should be interpreted as encompassing the security risks which could reasonably be judged to affect hardware, software and algorithms used by the DSRSP to deliver its services.

NOTE *For example, if the organization is delivering a web-based consumer support service, it would be reasonable to expect that the website has addressed known technical vulnerabilities including, for example, the Open Web Application Security Project's (OWASP) top 10 web application vulnerabilities. Further information is available at the OWASP website[6].*

10.7.3 Exercising supplier and supply chain due diligence

In respect of its DSR system, the DSRSP should establish, document and maintain system and configuration management records of the locations, premises, systems, software and master data used to deliver its DSR services, and, as a minimum, should comprise an overview of the:

a) DSRSP's current operations, to include:
   1) the locations/premises at which its personnel and systems operate;
   2) the DSRSP's ICT equipment and systems, including any outsourced or externally hosted components; and
   3) any DSR system-related assets;
b) types of products, systems and/or services that the DSRSP:
   1) has delivered;
   2) is currently delivering; and
   3) plans to deliver.

The above information should cover the lifecycle of the DSRSP's services and any supporting products, software and/or systems.

[6] Available at: https://owasp.org/.

Annex A (informative)
Relevant standards and other guidance mapped to clauses

The table below maps a number of relevant standards and other guidance documents to clauses in this PAS. The list is not exhaustive.

Table A.1 – Relevant standards and guidance mapped by clause

Clause	Standards and other guidance
6.2 Security governance	BS EN IEC 62443-3-2 BS EN ISO/IEC 27001 BS EN ISO/IEC 27019 BS EN ISO/IEC 27043 BS ISO/IEC 27010 BS ISO/IEC 27014 IEC 62443-2-1 IEC TS 62443-1-1 ISO/IEC 27005 PAS 1085:2018, Clauses **5**, **6** and **7** *CPNI Passport to good security for senior executives* [7] *CPNI Thinking securely abour your business*[7)] *NCSC Board toolkit* [6] *NCSC Cloud security guidance – Having confidence in cyber security* [17] *NCSC Risk management guidance – Component-driven and system-driven approaches* [18] *NCSC Risk management guidance – Introduction to security governance* [19] *NCSC Secure design principles – Establish the context before designing a system* [20]
6.3 Holistic approach to security	PAS 1085:2018
8.1 Data privacy: Practices to be adopted for provision of consumer DSR services	BS EN ISO/IEC 29100 PAS 185 PAS 1085:2018, Clause **11**
8.2 ESA manufacturer	PAS 1878:2021
8.3 Data and information sharing agreement	BS 10010 PAS 185 PAS 1085:2018, Clause **11**

[7)] Available at: https://www.cpni.gov.uk/secure-business.

Table A.1 – Relevant standards and guidance mapped by clause *(continued)*

Clause	Standards and other guidance
10.1 Cyber security practices to be adopted for provision of consumer response mode DSR services	ETSI EN 303 645 IEC 62443-2-1 IEC TS 62443-1-1
10.2 Personnel security	BS 7858
10.3 Supply chain security management	BS ISO/IEC 27010 PAS 1085:2018, Clauses **8** and **9**
10.4 Monitoring changes to threat landscape and emerging vulnerabilities	BS EN ISO/IEC 27019 BS EN ISO/IEC 27002 IEC 62443-2-1 *CREST Protective monitoring guidance* [21] *NCSC Introduction to logging for security purposes* [22] *NCSC 10 Steps to cyber security – Monitoring* [23] *NCSC Security operations centre (SOC) buyers guide* [24] *NCSC Secure design principles – Making compromise detection easier* [25] *NIST SP 800-137: Information security continuous monitoring* [26] *NIST SP 800-94: Guide to intrusion detection and prevention systems (IDPS)* [27]
10.5 Communications, data and information security	BS EN ISO/IEC 27001 IEC TS 62443-1-1
10.6 Security of CEM and ESA components employed in delivery of DSRSP's services	ETSI EN 303 645
10.7 Secure-by-design	ETSI EN 303 645

Annex B (informative)
Trust modelling

*COMMENTARY ON **ANNEX B***

This Annex is informative, illustrative and non-exhaustive. The trust relationships are currently only illustrative and limited in scope, so can only be used as examples of what future trust models might look like.

The trust models have not been used to derive security related consequences and are informative only; currently no security recommendations in this PAS and PAS 1878:2021 have been mapped to the trust models, i.e. there is no link between the two and therefore none can be inferred.

B.1 Introduction

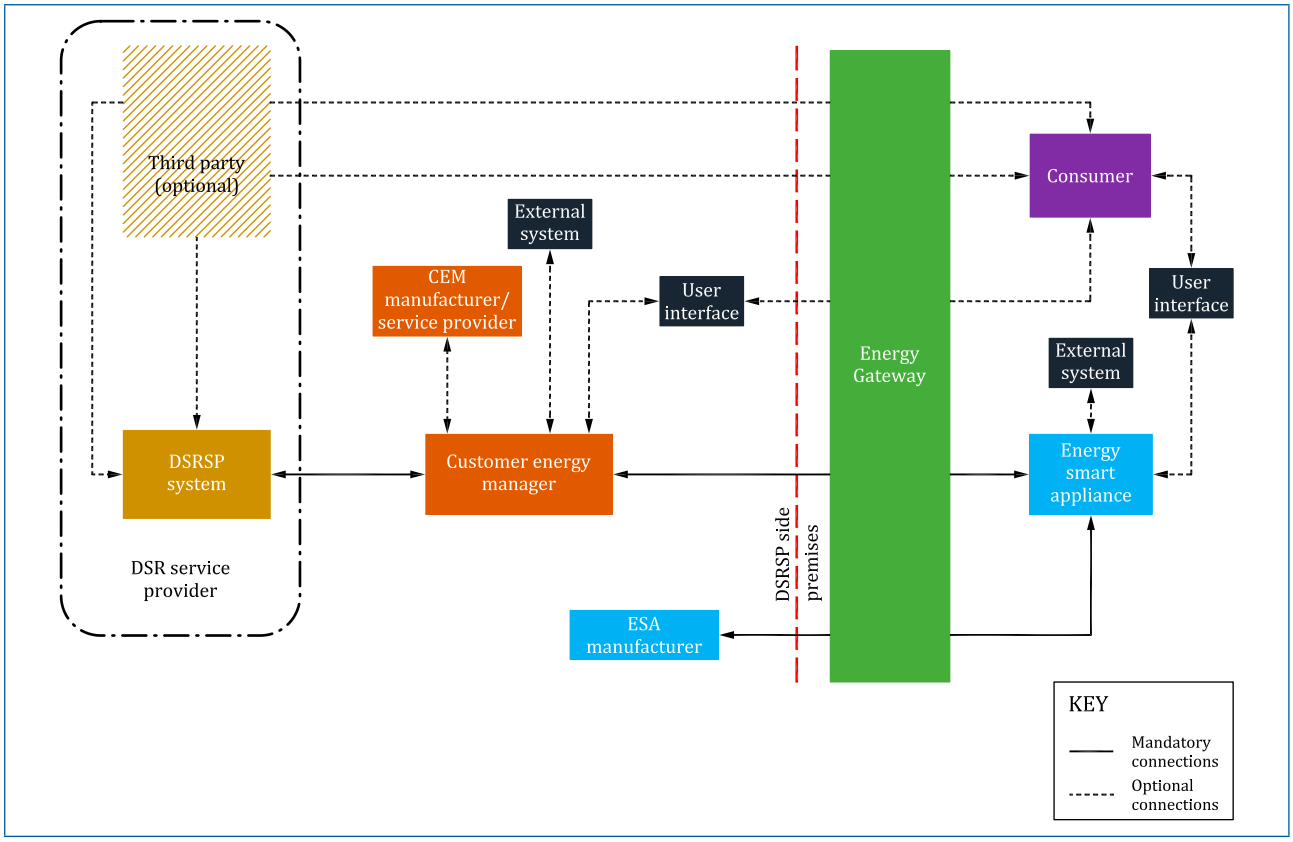
The illustrative trust models in this Annex were developed in respect of the implementation of a cloud-based CEM architecture for the DSR management of electricity supply. They are based on the DSR approach outlined in PAS 1878 (Energy smart appliances) and PAS 1879 (DSR service provision). The trust models illustrate the nature of the trust relationships in a generic architecture and may be used to inform the development of specific security measures.

This Annex provides a brief overview of the trust modelling work, before focusing specifically on the initialization process. The initialization process was chosen as an initial example to demonstrate trust modelling concepts.

B.2 Scope

The scope of the trust modelling is illustrated in Figure B.1, and the components and their functionality are described in PAS 1878:2021.

Figure B.1 – High level functional architecture for DSR



B.3 High-level view of DSR service lifecycle

The lifecycle comprises the following generic stages:

- registration;
- initialization;
- DSR service operations; and
- deregistration of the ESA.

B.4 Trust model for the initialization process

B.4.1 Overview

The trust model for the initialization process comprises the following steps, which are outlined in more detail below:

- DSRSP provides consumer with DSR service initialization information;
- consumer obtains access to ESA configuration settings via user interface;
- consumer establishes ESA connectivity to Energy Gateway (e.g. broadband router);
- ESA connects to its manufacturer and downloads/applies any available patches;
- consumer establishes ESA connectivity to cloud-based CEM;
- consumer identifies required DSRSP to CEM via one of the user interfaces (ESA or CEM);
- CEM establishes connection to DSRSP;
- ESA establishes connectivity to DSRSP via the CEM;
- consumer submits service initialization information to register ESA with DSRSP;
- DSRSP and ESA perform initialization information exchanges; and
- ESA is initialized and ready to enter DSR service operations.

B.4.2 DSRSP provides consumer with DSR service initialization information

The DSRSP provides the consumer with the initialization information for an ESA.

As part of the registration process, the consumer will have created an account with the DSRSP or a third party acting on behalf of the DSRSP, and in doing so established a means of receiving the initialization information.

The consumer trusts:

- that the DSRSP will be available when required, so the DSRSP can provide the initialization information to them;
- in the identity of the DSRSP, so that they know they are interacting with a legitimate DSRSP;
- in the means by which they communicate with the DSRSP, so that the information sent and received cannot be viewed or altered by a third party;
- in the means by which the DSRSP stores and processes their data, so that privacy and accuracy are maintained; and
- that the initialization information provided by the DSRSP is correct, complete and unaltered, so that the initialization process can be completed.

The DSRSP trusts:

- in the identity of the consumer with whom it is communicating, so that it can associate the ESA with the correct consumer account;
- in the means by which it communicates with the consumer, so that the information sent and received cannot be viewed or altered by a third party;
- that the data provided by the consumer is correct, complete and unaltered, so that it can be used effectively by the DSRSP;
- that the initialization information provided by the consumer is correct, complete and unaltered, so that the initialization process can be completed;
- that it can uniquely identify each consumer supply point so that the DSR operation can be applied to known electricity distribution network locations; and
- that it can uniquely identify each enrolled ESA, so that the DSR operation can be applied to a specified ESA.

B.4.3 Consumer obtains access to ESA configuration settings via user interface

Using the mechanism provided by the ESA manufacturer, the consumer accesses the ESA's user interface.

The consumer trusts:

- that their ESA's user interface will be available when required, so it can process the initialization information provided by the consumer;
- in the means of identifying and communicating with the ESA via its user interface, so that the information sent and received is to the right location and cannot be viewed or altered by a third party;

- that the information displayed by their ESA's user interface is correct, complete and unaltered, so that the initialization process can be completed;
- that their ESA's user interface is not communicating with third parties without the consumer's consent, so that privacy can be maintained;
- that their ESA operates within the constraints of only those services and data exchanges required for DSR that the consumer has requested or configured; and
- that unauthorized parties cannot modify their ESA's setup, configuration or operation.

The ESA's user interface trusts:

- in the means by which it communicates with the consumer, so that the information sent and received cannot be viewed or altered by a third party;
- that the information supplied by the consumer is correct, complete and unaltered, so that the initialization process can be completed; and
- in the identity of the consumer, so that the consumer's privacy is maintained and DSR interventions are associated with the correct consumer account.

B.4.4 Consumer establishes ESA connectivity to the Energy Gateway (e.g. broadband router)

Using the ESA's user interface, the consumer provides the local configuration information required to connect the ESA to the Energy Gateway. The local configuration information can, for example, be the network identity and password or similar credentials required to establish a connection to the Wi-Fi network in the consumer's premises. In **B.4.3,** the consumer established trust relationships with the ESA via the ESA user interface, thereby allowing initial configuration of the ESA. Having established this connectivity, the consumer connects the ESA to the premises area network (e.g. the home Wi-Fi) so that the ESA can establish a connection to the CEM and then to the DSRSP.

The consumer trusts:

- that their ESA and Energy Gateway will be available when required, so that the ESA can process the network connection information sent to it;
- in the authenticity of their ESA, so that the consumer knows they are interacting with a legitimate ESA;
- in the means by which their ESA stores and processes the network connection information, so that privacy and accuracy are maintained;
- in the means by which their ESA communicates with their Energy Gateway, so that the network connection information sent and received cannot be viewed or altered by a third party;
- that their ESA will not interfere with the operation of other devices and ESAs in their premises that are connected to their Energy Gateway, so that the availability and integrity of the other devices and/or appliances are not compromised; and
- that their ESA will not permit unauthorized access to the network connection information provided by the consumer, so that their privacy is maintained.

The Energy Gateway trusts:

- in the means of communicating with the ESA, so that the information sent and received cannot be viewed or altered by a third party; and
- that the initial connection request is from a legitimate ESA and was authorized by the consumer.

B.4.5 ESA connects to its manufacturer's update service to download/apply any available patches

On initial connection to the internet, the ESA will connect to its manufacturer's update service. It will then download, verify and apply any available patches. The term patch is used to encompass any updates to the software or firmware in the ESA provided by the manufacturer or its authorized agent.

The consumer trusts that:

- the manufacturer's update service will be available when required so that any required patches can be successfully downloaded;
- their ESA will download and apply any required patches so that the security, performance and availability of their ESA is maintained;
- the ESA manufacturer will only provide authentic patches that are compliant with the requirements of PAS 1878:2021;
- the ESA manufacturer will be available to investigate and resolve potential patch issues causing pressing problems (for example, to minimize the time for which their ESA is exposed to known threats);
- once deployed, the patches do not affect the confidentiality of information processed on their premises network, so that the consumer's privacy is maintained; and
- once deployed, the patches will not adversely affect the operation of any other devices and ESAs on their premises network, so that their availability and integrity are not compromised.

The ESA trusts:

- that its manufacturer's update service will be available when required, so it can download any updates to the software or firmware;

- in the identity of its manufacturer's update service, so that the ESA knows it is interacting with the legitimate manufacturer's update service;
- in the means by which the ESA communicates with its manufacturer's update service, so that the information sent and received cannot be viewed or altered by a third party; and
- that any software or firmware updates received from its manufacturer's update service are complete, correct and unaltered, so that the update process can be successfully completed without impacting the existing security of the ESA.

B.4.6 Consumer establishes ESA connectivity to cloud-based CEM

Once the ESA has applied any available patches, the consumer, or the ESA, then initiates a connection to the cloud-based CEM.

The consumer trusts:

- that their ESA will be available when required, so it can process the CEM connection information sent to it;
- in the authenticity of their CEM, so that the consumer knows they are interacting with a legitimate CEM;
- in the means by which their ESA stores and processes the CEM connection information, so that privacy and accuracy are maintained;
- in the means by which their ESA communicates, via their Energy Gateway, with the CEM so that the network connection information sent and received cannot be viewed or altered by a third party and its accuracy is maintained; and
- that the CEM will not permit unauthorized access to the network connection information provided by the consumer, so that their privacy is maintained.

The CEM trusts:

- in the means of communicating with the ESA, so that the information sent and received cannot be viewed or altered by a third party; and
- that the initial connection request is from a legitimate ESA and was authorized by the consumer.

B.4.7 Consumer identifies required DSRSP to CEM via one of the user interfaces (ESA or CEM)

Once the ESA has connected to the CEM, the consumer can identify which DSRSP the CEM connects to. The consumer will achieve this through a user interface, which might be to the ESA or to the CEM. The consumer uses the service initialization information provided by the DSRSP to initiate a connection from the CEM to the DSRSP.

__NOTE__ If the UI employed by the consumer is via the ESA, the trust relationships in __B.4.3__ apply, if it is direct to the CEM a similar set of trust relationships are required for the user interface to CEM connection.

The consumer trusts:

- that their CEM will be available when required, so it can process the DSRSP connection information provided by the consumer;
- in the means by which their CEM stores and processes the service initialization information, so that privacy and accuracy are maintained; and
- that the CEM will not permit unauthorized access to the service initialization information provided by the consumer, so that their privacy is maintained.

The CEM trusts:

- in the means of communicating with the consumer user interface, so that the service initialization information sent and received cannot be viewed or altered by a third party; and
- that the service initialization request is from a legitimate consumer to whom the DSRSP provided the service initialization information.

B.4.8 CEM establishes connection to DSRSP

Using the service initialization information provided by the consumer the CEM initiates and establishes a connection to the selected DSRSP.

The consumer trusts:

- that the DSRSP will be available when required, so that the CEM can connect to the DSRSP;
- in the means by which their CEM stores and processes the service initialization information, so that privacy and accuracy are maintained;
- in the means by which their CEM communicates with the DSRSP so that the service initialization information sent and received cannot be viewed or altered by a third party and its accuracy is maintained; and

- that the DSRSP will not permit unauthorized access to the service initialization information used by the CEM, so that their privacy is maintained.

The CEM trusts:

- that the service initialization information provided by the consumer is accurate and complete.

The DSRSP trusts:

- in the means of communicating with the CEM, so that the service initialization information sent and received cannot be viewed or altered by a third party; and
- that the service initialization request is from a legitimate consumer to whom it provided the service initialization information.

B.4.9 ESA establishes connectivity to DSRSP via the CEM

Once the CEM has successfully connected to the DSRSP, the ESA establishes communications connectivity to the DSRSP (i.e. an end-to-end connection test via the CEM).

The ESA trusts:

- that it is communicating with the DSRSP with which the consumer has registered; and
- that the end-to-end communications over which information is sent and received cannot be viewed or altered by a third party and its accuracy is maintained.

The DSRSP trusts:

- that it is communicating with a genuine ESA; and
- that the end-to-end communications over which information is sent and received cannot be viewed or altered by a third party and its accuracy is maintained.

B.4.10 Consumer submits service initialization information to register ESA with DSRSP

If not already provided via the user interface, the consumer provides the service initialization information. The DSRSP registers the ESA associating it with the consumer's account.

The consumer trusts:

- in the identity of the DSRSP with which the ESA is communicating; and
- that the accuracy of the service initialization information will be maintained when stored and processed by the DSRSP so that the ESA is correctly associated with their account.

The DSRSP trusts:

- in the identity of the ESA with which it is communicating;
- that the service initialization information it has received was provided to the consumer that is initiating the ESA registration; and
- that the service initialization information provided by the ESA is correct, complete and unaltered.

B.4.11 DSRSP and ESA perform initialization information exchanges

The DSRSP and ESA perform the initialization activities as specified in PAS 1878:2021. As part of these exchanges the DSRSP may test the ESA's response to service requests.

The consumer trusts:

- information provided by the DSRSP, including any service requests, will not interfere with the planned operation of the ESA except as permitted by the consumer's flexibility preferences.

The ESA trusts:

- information provided by the DSRSP, including any service requests, will not modulate the planned operation of the ESA, except as permitted by the consumer's flexibility preferences.

The DSRSP trusts:

- information provided by the ESA is correct, complete and unaltered, except as legitimately altered by the CEM in accordance with the consumer's preferences.

B.4.12 ESA is initialized and ready to enter DSR service operations

The initialization process is complete, with communications established between the ESA and the DSRSP via the CEM.

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 7858, *Screening of individuals working in a secure environment – Code of practice*

BS 10010, *Information classification, marking and handling – Specification*

BS EN IEC 62443-3-2, *Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design*

BS EN ISO 9000, *Quality management systems – Fundamentals and vocabulary*

BS EN ISO 19650-5:2020, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) – Information management using building information modelling – Part 5: Security-minded approach to information management*

BS EN ISO/IEC 27000:2020, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

BS EN ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013)*

BS EN ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013)*

BS EN ISO/IEC 27019, *Information technology – Security techniques – Information security controls for the energy utility industry*

BS EN ISO/IEC 27043, *Information technology – Security techniques – Incident investigation principles and processes (ISO/IEC 27043:2015)*

BS EN ISO/IEC 29100, *Informating technology – Security techniques – Privacy framework*

BS ISO/IEC 27010, *Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications*

BS ISO/IEC 27014, *Information security, cybersecurity and privacy protection – Governance of information security*

IEC TS 60364-8-3:2020, *Low-voltage electrical installations – Part 8-3: Functional aspects – Operation of prosumer's electrical installations*

ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*

PAS 185, *Smart Cities – Specification for establishing and implementing a security-minded approach*

PAS 1085:2018, *Manufacturing – Establishing and implementing a security-minded approach – Specification*

PAS 7040:2019, *Digital manufacturing – Trustworthiness and precision of networked sensors – Guide*

Other publications

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

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

[3] ELEXON. *Balancing and settlement code.* Available at: https://www.elexon.co.uk/bsc-and-codes/balancing-settlement-code/.

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

[5] EUROPEAN COMMUNITIES. Regulation (EU) 2016/679. Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive). Luxembourg: Office for Official Publications of the European Communities, 2018.

[6] NATIONAL CYBER SECURITY CENTRE. *Board toolkit.* NCSC, 2019. Available at: https://www.ncsc.gov.uk/collection/board-toolkit.

[7] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Passport to good security for senior executives.* CPNI, 2019. Available at: https://www.cpni.gov.uk/managing-my-asset/leadership-in-security/board-security-passport.

[8] NATIONAL CYBER SECURITY CENTRE. *Incident management*. NCSC, 2019. Available at: https://www.ncsc.gov.uk/collection/incident-management.

[9] GREAT BRITAIN. Network and Information Systems Regulations 2018. London: The Stationery Office.

[10] NATIONAL CYBER SECURITY CENTRE. *Top tips for staff*. NCSC, 2020. Available at: https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available.

[11] NATIONAL CYBER SECURITY CENTRE. *Phishing attacks: Defending your organisation*. NCSC, 2018. Available at: https://www.ncsc.gov.uk/guidance/phishing.

[12] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *NIST SP 800-161: Supply chain risk management practices for federal information systems and organizatons.* NIST, 2015. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[13] NATIONAL CYBER SECURITY CENTRE. *Supply chain security guidance.* NCSC, 2018. Available at: www.ncsc.gov.uk/guidance/supply-chain-security.

[14] NATIONAL CYBER SECURITY CENTRE. *Using TLS to protect data.* NCSC, 2017. Available at: https://www.ncsc.gov.uk/guidance/tls-external-facing-services.

[15] NATIONAL CYBER SECURITY CENTRE. *Using IPsec to protect data.* NCSC, 2016. Available at: https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data.

[16] DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT. *Secure-by-design report*. Department for Digital, Culture, Media and Sport, 2018. Available at: https://www.gov.uk/government/publications/secure-by-design-report.

[17] NATIONAL CYBER SECURITY CENTRE. *Cloud security guidance – Having confidence in cyber security.* NCSC, 2018. Available at: https://www.ncsc.gov.uk/collection/cloud-security/having-confidence-in-cyber-security.

[18] NATIONAL CYBER SECURITY CENTRE. *Risk management guidance – Component-driven and syster-driven approaches.* NCSC, 2016. Available at: https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches.

[19] NATIONAL CYBER SECURITY CENTRE. *Risk management guidance – Introduction to security governance.* NCSC, 2016. Available at: https://www.ncsc.gov.uk/collection/risk-management-collection/governance-cyber-risk/security-governance-introduction.

[20] NATIONAL CYBER SECURITY CENTRE. *Secure design principles – Establish the context before designing a system.* NCSC, 2019. Available at: https://www.ncsc.gov.uk/collection/cyber-security-design-principles/establish-the-context-before-designing-a-system.

[21] CREST. *Cyber security monitoring and logging guide*. CREST, 2015. Available at: https://www.crest-approved.org/wp-content/uploads/Cyber-Security-Monitoring-Guide.pdf.

[22] NATIONAL CYBER SECURITY CENTRE. *Introduction to logging for security purposes*. NCSC, 2018. Available at: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.

[23] NATIONAL CYBER SECURITY CENTRE. *10 steps to cyber security – Monitoring.* NCSC, 2019. Available at: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/monitoring.

[24] NATIONAL CYBER SECURITY CENTRE. *Security operations centre (SOC) buyers guide.* NCSC, 2016. Available at: https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide.

[25] NATIONAL CYBER SECURITY CENTRE. *Secure design principles – Make compromise detection easier.* NCSC, 2019. Available at: https://www.ncsc.gov.uk/collection/cyber-security-design-principles/making-compromise-detection-easier.

[26] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *NIST SP 800-137: Information security continuous monitoring (ISCM) for federal information systems and organizations.* NIST, 2011. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

[27] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *NIST SP 800-94: Guide to intrusion detection and prevention systems (IDPS).* NIST, 2007. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf.

Further reading

BS EN 50631-1, *Household appliances network and grid connectivity – Part 1: General requirements, generic data modelling and neutral messages*

BS IEC 62746-10-1, *Systems interface between customer energy management system and the power management system – Part 10-1: Open automated demand response*

NATIONAL CYBER SECURITY CENTRE. *Cyber assesment framework*. NCSC, 2019. Available at: https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework.

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

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

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

9 780539 051308