

**CENELEC/ICT**

Date: 200X-XX-XX

**CWA XXX-1**

Secretariat : NSB Member

## **Title – Interoperability Framework Requirements Specification**

ICS: <the ICS numbers will be provided by CEN at the time of publication>

Descriptors: To be added

### **Some comments:**

This title page will be replaced by the CWA Formal Title Page, created by the CENELEC Standards Delivery Department at the moment of producing the CWA for publication. Users of this template can therefore use the title page to contain any information they wish.

What is important is that the CWA content itself starts, after a section break, in a new section, with a contents table, which should be automatically generated.

Considering that the draft CWA will undergo various revisions in the Workshop before being ready for publication, it is perfectly OK to adapt the CWA reference in the Header to contain the working document reference. It is only the final draft that should contain the CWA reference in the Header. Note however that in current practice, the CWA reference number is allocated at the time of publication by the CENELEC Standards Delivery Department.

**NOTE: ANY TEXT IN RED (SUCH AS THIS TEXT) REMAINS AS AN INSTRUCTION TO THE EDITORS AND WILL NOT FORM PART OF THE FINAL CWA**

For questions and comments, please contact [operations@cenelec.eu](mailto:operations@cenelec.eu)

**Contents**

1

2

3 **Contents ..... 2**

4 **Foreword ..... 3**

5 **Introduction..... 4**

6 **1. Scope ..... 5**

7 **2. Normative References..... 6**

8 **3. Definitions, symbols and abbreviations..... 8**

9 **4. Conformance clauses ..... 16**

10 **Annex A Informative Annexes..... 22**

11 A.1 Use Cases..... 22

12 **Annex B (Normative) : Interoperability Implementation Conformance Statement Proforma ..... 30**

13 **B.1 Scope ..... 30**

14 **B.2 References..... 30**

15 **B.3 Definitions and abbreviations..... 30**

16 **B.4 Requirements for Conformance to this IICS ..... 30**

17 **B.5 Instructions for Completion of the IICS..... 30**

18 **B.6 Global Statement of IICS Conformance..... 31**

19 **Bibliography ..... 31**

**Document History (to be removed in final document)**

20

21

Document	Version	Date	filename
Internal Working Draft Version	1.9	16/12/2008	IFI Requirements Specification 16-12-13-Draft-V-1.9.doc
Draft Version for informal comment	2.0	18/12/2008	IFI Requirements Specification 2008-12-18-Draft-V-2.0.doc
Draft Version updated with SP input and copied in Chen input	2.1	11/02/2009	IFI Requirements Specification 2008-12-18-Draft-V-2.1.doc
Draft Version updated during Teleconference 12/01/2009	2.2	12/01/2009	IFI Requirements Specification 2008-12-18-Draft-V-2.2.doc
Draft Version updated during and subsequent to Teleconferences 15/01/2009	2.3	15/01/2009	IFI Requirements Specification 2008-12-18-Draft-V-2.3.doc
Draft Version updated during and subsequent to Teleconferences 15/01/2009	2.3a	15/01/2009	IFI Requirements Specification 2008-12-18-Draft-V-2.3a.doc
Final Draft Version prior to submission to TAHI Board	2.4	19/01/2009	IFI Requirements Specification 2008-12-18-Draft-V-2.4.doc
Board Agreed Version for distribution by NSB	2.5	28/01/2009	IFI Requirements Specification 2008-12-18-Draft-V-2.5.doc
First Review Comments integrated for rev2	3.1	27/09/2009	IFI Requirements Specification 2008-12-18-Draft-V-3.1.doc
Issued in CWA format with Comments Integrated with Line Numbers editing document	CWA V1.0	01/10/2009	CENELEC CWA 4 IFRS V1.0.doc
Issued in CWA format with Comments Integrated with Line Numbers for Comment	CWA V1.0	01/10/2009	CENELEC CWA 4 IFRS V1.0.pdf

22 **Foreword**

23

24 <What follows is a template text for a typical Foreword. You can adjust the text to your Workshop's  
25 circumstances. Unlike the rest of the CWA, this text will be checked by CENELEC before publication.  
26 CENELEC may decide to add paragraphs to it which it considers necessary in the context of providing full  
27 transparency on what the CWA and its process>

28

29 Editor's Note: some suggestions made in the text below.

30

31 The production of this CWA (CENELEC Workshop Agreement) specifying Interoperability Framework  
32 Requirements for electronic systems in homes and buildings, was formally accepted at the Workshop's kick-  
33 off meeting on 2009-07-07.

34 The document has been developed through the collaboration of a number of contributing partners in the  
35 Workshop. This CWA has received the support of representatives of each of these contributing partners.  
36 Information on who have supported the document's contents may be obtained from the CENELEC  
37 Management Centre.

38 CWA approval was obtained at the Workshop's meeting on 2009-07-07.

39 This CWA consists of a single part, this document, under the general title *Interoperability Framework*  
40 *Requirements Specification*:

41

**Foreword**

The Foreword is always the first unnumbered clause.

Normally it is drafted by the CENELEC Management Centre, but certain paragraphs in the Foreword can also be the subject of prior discussion in the Workshop. The Foreword can in any case contain elements specific to the Workshop.

In the case of a multi-part CWA, the Foreword will refer to the other parts

42

43 **Introduction**

44  
45 One aspect of the vision of the intelligent home has not changed over its cycles of renewal: that open,  
46 generative, standard technology platforms that can be configured to support many services will replace  
47 hardwired, proprietary, appliances that provide one specific service. Devices that participate in these  
48 platforms will *interoperate*: they will exchange information and act upon it in a consistent way with the  
49 possible assistance of *interworking* functions that route and manipulate information without affecting its  
50 semantics, to bridge discontinuities of media, technology or administration.

51  
52 Interworking functions will evolve in various ways in response to changing technology, media, products and  
53 standards. They will be largely under the control of system designers, solution builders and installers; and  
54 invisible to the end user, embedded in gateways, STBs and other forwarding/switching points.

55  
56 Interoperability, its successes and failures, by contrast is a highly visible property of the elements of a system  
57 and one that requires continual review and renewal at great expense of time and effort. The Interoperability  
58 Framework Requirements Specification (IFRS) CWA is motivated by the need to set formal expectations of  
59 the likelihood of such success or failure and help designers, implementers and installers to make informed  
60 choices.

61  
62 Accordingly, this IFRS CWA defines a set of requirements that a technical specification for an object should  
63 fulfil in order to enable a general interoperability framework for home and building electronic service systems.

64  
65 The objective is to allow installers, system integrators and service providers to identify equipment and  
66 devices that may be deployed in customer premises and utilise them in new applications and services  
67 regardless of the underlying communication protocol or home system the devices use. In order to do this  
68 there is inherent in these requirements a set of conditions that services and applications utilising this  
69 specification must observe in order to obtain interoperability.

70  
71 There are already many existing systems and protocols supported by major organisations and these have  
72 been developed over many years and are stable products. Some are already International Standards. Some  
73 are already widely deployed. The organisations that support and promote these systems have defined rules,  
74 guidelines and practices that ensure that products are interoperable.

75  
76 The expectation is that new protocols for interacting between devices using one or more of these systems  
77 and protocols will be developed. This specification aims therefore to ensure that the requirements it proposes  
78 are compatible with those used by existing or future systems, that lie within the scope of this framework and  
79 where these are designed to interact with systems or devices that are external to them.

80  
81 In particular, this specification will ensure that any existing system can deliver information and execute  
82 interactions at its boundary with other systems in an interoperable format:

- 83  
84 (i) the identity of any object or device within its system boundary that it wishes interact with interoperably in  
85 the context of this specification; alongside  
86 (ii) methods for discovering such an object together with its specification; accompanied by  
87 (iii) the methods of configuring and managing that object; and  
88 (iv) the application, or service, specific interactions between the object and others.

89  
90 This vision of devices and services interacting to form new applications across application and system  
91 domains may result in multiple applications or services requiring access and control of individual devices and  
92 objects in the premise (i.e. domains, applications and systems will intersect). Therefore this document will  
93 address the requirements for safety, security and priority of access and control in as much as they affect, or  
94 are affected, by the interoperability requirements.

95  
96 The implementation of this specification/standard can be seen as a solution which facilitates middleware.  
97 Although it recognises that a number of solutions exist already for some applications, this standard does not  
98 make recommendations for any particular solutions, rather it sets out the requirements that must be met to  
99 ensure they are interoperable in this domain

100 **1. Scope**

101

102 The scope of the IFRS applies to any object (understood to be defined in a variety of ways, such as: device,  
103 equipment, sensor, actuator, network, protocol, application, service) that may be utilised in buildings,  
104 premises and particularly in the domestic environment. (It is seen that this specification could apply to many  
105 other environments). This standard does not state or suggest how the Interoperability Framework should be  
106 implemented as this is seen as the remit of the many developers and organisations active in the field and the  
107 means of delivering a fully specified general Interoperability Framework should be the subject of future  
108 development work.

109

110 <May need more input>

111

112  
113**2. Normative References**

Publications	Standard	Responsible body (input from)	Status
1	ISO/IEC 18012-1:2004 Information technology -- Home Electronic System -- Guidelines for product interoperability -- Part 1: Introduction	ISO/IEC JTC 1/SC 25	IS
1	ISO/IEC 18012-2:xxxx Information technology -- Home Electronic System -- Guidelines for product interoperability -- Part 2: Taxonomy and Lexicon	ISO/IEC JTC 1/SC 25 WG1	Work in progress (FCD)
1	ISO/IEC 14543-2-1 Part 2-1: Introduction and device modularity (EN 50090)	ISO/IEC JTC 1 SC25	IS
5	ISO/IEC 14543-3-x (5 parts) EN 50090 Series	ISO/IEC JTC 1 SC25 CENELEC TC205	IS
4	ISO/IEC-14908-x (4 parts)	ISO/IEC JTC 1 SC25 CEN TC247	IS being published
1	ISO/IEC 29341-2:2008 Information technology -- UPnP Device Architecture -- Part 2: Basic Device Control Protocol - Basic Device	ISO/IEC JTC 1/SC 25	IS
1	ISO/IEC 29341-1:2008 Information technology -- UPnP Device Architecture -- Part 1: UPnP Device Architecture Version 1.0	ISO/IEC JTC 1/SC 25	IS
72	ISO/IEC 29341-x-y (72 parts)	ISO/IEC JTC1 SC25	IS
?	ANSI CEBus	ANSI	
2	ISO/IEC 14543-4-1 & -2	ISO/IEC JTC1 SC25 (ECHONET Association <a href="http://www.echonet.gr.jp">http://www.echonet.gr.jp</a> )	IS Industry Association
7	ISO/IEC 14543-5-x (7 drafts)	ISO/IEC JTC1 SC25 (IGRS Alliance)	Work in progress
1	CENELEC Smart House CoP	CEN/CENELEC	WA
1	IEC 62481-1 Digital Living Network Alliance (DLNA) Home Networked Device Interoperability Guidelines - Part 1: Architecture and Protocols	IEC TC100	IS
?	CECED	CENELEC TC59X	Work in progress
?	BACNET	ISO TC 205	IS
?	ZigBee	IEEE 802.15.4 - 2003	
2	LonWorks Interoperability Profiles Functional Profiles	CEN 14908-5 & -6 (LonWork Association ( <a href="http://www.lonworks.org">http://www.lonworks.org</a> ))	Work in progress

114  
115  
116**Normative References**

This **optional** element shall give a list of any normative documents to which reference is made in the CWA in

such a way as to make them indispensable for the application of the CWA. For dated references, each shall be given with its year of publication, or, in the case of enquiry or final drafts, with a dash together with a footnote "To be published", and full title. The year of publication or dash shall not be given for undated references. When an undated reference is to all parts of a standard, the publication number shall be followed by the indication "(all parts)" and the general title of the series of parts (i.e. the introductory and main elements).

It is suggested to start as follows: "The following normative documents contain provisions which, through reference in this text, constitute provisions of this CWA. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this CWA are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies." In case of a CWA that is containing informational material only, there are no Normative references. The references are in that case to be listed as "Informative references" in an Annex (see below). In addition, a CWA can contain both Normative AND Informative References.

In addition to these references, which are actually referenced somewhere, there may also be added a Bibliography (see below)

Examples are given below:

ISO 1234-1, Example Standard Reference - Part 1: First example

ISO 12345-1999, Second Example Standard Reference

ISO 6789, Third Example Standard - A non-published one, - <sup>1</sup>

**Note that normative references may be made not only to publications of formal standards bodies. For example, reference may be made to consortia specifications, provided these are publically available.**

---

<sup>1</sup> To be published

118  
119  
120  
121  
122  
123  
124

### 3. Definitions, symbols and abbreviations

[NOTE : Title will have to be amended based upon the subsections that are present]

#### 3.1 Definitions

##### 3.1.1 General Definitions

<b>Application</b>	<p>A collection of Functions that have measurable effects on the physical world and are used by people to achieve objectives consistent with the specified capabilities of the Application. An Application is composed from many of the items defined below. In particular it may include Services, made available under Service Level Agreements by Service Providers, that themselves are composed of Applications.</p> <p>Note: the distinction between Application and Service is made for the purposes of this CWA.</p> <p>Example: devices in the Smart House collaborate to execute an energy management Application that the Owner uses to reduce electricity consumption. No Service is required.</p>
<b>Application / Object Service</b>	<p>A function provided through a well-defined API by a device or object to another device or object.</p> <p>Example: getting a temperature value, arming the alarm system, etc.</p>
<b>Building</b>	<p>A man-made structure with an interior, an exterior boundary, and an owner. By this definition a building may be composed of a collection of buildings.</p> <p>Example: a house (owner-occupied or rented), a block of flats, a hotel (containing rooms or suites whose occupants have temporary ownership), a station. Could also be a car or other vehicle.</p> <p>Example: a business located at several sites; multiple buildings with a single owner. The interconnection provides for communication between management systems, hence a potential interoperability issue.</p>
<b>Consumer</b>	<p>Any natural person who uses, requests or purchases products and services. For the purposes of this document the “consumer” is considered to be the end user of smart house technology.</p> <p>Example: the occupant of a smart house and any visitors. In fact any people at home. Note: consumers differ in their abilities and the different requirements are an aspect of interoperability, e.g. when a motor-impaired consumer interacts with an installed system.</p>
<b>Customer</b>	<p>A person or organisation who contracts with any entity in order to design, install or maintain a smart house system or to use any service or application provided by a service provider to the end-user or consumer in the smart house.</p> <p>Example: a consumer as defined above may be a customer. A company that sub-contracts the management of its building is a customer of the service provider (defined below).</p>
<b>Device</b>	<p>An electronic object comprising instances of sensing and/or actuation and/or communications functions implementing them on behalf of one or more owners. It may be a Product in its own right or part of a Product together with other Devices. See also Device Object.</p> <p>Example: a proximity detector that activates a light by direct power switching and also sends a message to a security system to alert it that a person (or an animal) is nearby. This is a Product and also part of a larger Product that is the security system.</p>
<b>End User</b>	<p>Any natural person who is the user of equipment or recipient of services in the home environment</p> <p>Example: the children in a household, who are neither Consumers nor Customers according to the definitions above.</p>
<b>Function</b>	<p>The collection of instructions that process information and communicate it to other functions with measurable effects. A function may be a collection of one or more functions.</p> <p>Example: a thermostat, whose function is a capability to monitor ambient temperature against thresholds set by End Users. Such a function may reside in a variety of locations depending on system, application or service architecture and actual installation. For example, it might be implemented in an energy manager in an End User’s personal communicator or computer, or a smart meter, that polls, or receives, values from temperature sensors; or in a multi-function thermostat that receives thresholds from a controller, monitors them locally and notifies other functions when they are exceeded. The distribution of functionality, the information flows and locus of control will vary accordingly.</p>

<b>Home</b>	<p>Premises in which a person lives (or people live) and are the identified people that live in that particular building.</p> <p>Example: a house, an apartment in a block of flats, farm or estate comprising a house and outbuildings.</p>
<b>Instance</b>	<p>An object or service embodied in a product that possesses an identity and one or more owners and that may originate and or respond to events external to it.</p> <p>Example: the thermostat described above following its integration into a working installation, which implies acquisition of an identifier such as a network address and references to its internal objects.</p>
<b>Network</b>	<p>A collection of devices that are connected together for the exchange of data and sharing of resources. It is characterised by a collection of identifiers with one or more owners. The term "Address" is usually used to refer to such identifiers.</p> <p>Example: the Internet sub-network numbers and sub-network masks (or prefixes) constituting the Autonomous System (AS) assigned to an ISP or other operator of Internet services.</p> <p>Example: a collection of telecare devices installed in a Consumer's Premises that have discovered each other, configured automatically as a network, acquiring network addresses, and have registered through a gateway with a Service Provider.</p>
<b>Owner</b>	<p>A legal entity that may define access rights, authorisation, authentication, service level agreements, and policies and may delegate those from time to time.</p> <p>Note: A Consumer will often be an Owner. An End User may not be an Owner, i.e. it has no authority to define, or delegate the elements listed above.</p> <p>Example: an individual who installs and manages a collection of objects that implement applications ; a service provider that offers a service under a service level agreement to manage a collection of objects on behalf of other owners.</p>
<b>Policy</b>	<p>A collection of conditional instructions that allow, or deny, the execution of operations on objects.</p> <p>Example: if time of day before 0830 UTC then heating on; if the cat at the cat-flap is ours then let it in. The combinations of such policies form an interoperability issue.</p>
<b>Premises</b>	<p>One or more buildings with one or more owners, whose exterior boundaries may be interconnected by ICT networks.</p> <p>Example: for multiple building premises would be a business located at several sites, or multiple buildings with a single owner. The interconnection provides for communication between management systems, hence a potential interoperability issue.</p>
<b>QoS</b>	<p>The requesting and delivery of specific, quantifiable performance levels on a shared network or on services delivered. Typical QoS parameters include: throughput, loss, latency (or delay), response time, and jitter to describe a network's performance in the treatment of specific classes of data.</p> <p>Example: a security system must have a throughput of 300 bps, 0% loss, 200 ms response time.</p>
<b>Schema</b>	<p>Schema defines the structure and contents of any information resource. As a data catalogue for a database, a schema identifies the entities and the types of attributes for those entities. A schema for an enterprise may also define rules of use and legal values.</p> <p>Example: an XML schema defines the structure of an XML document. An XML schema defines things such as which data elements and attributes can appear in an object (such as a document or application) and how the data elements relate to one another.</p>
<b>Service</b>	<p>A product or good provided by a Service Provider to a consumer.</p> <p>In the Smart House many of these will be provided through electronic systems that regulate the home or provide entertainment, healthcare, security or safety in the home.</p> <p>In this context a service is delivered by a service application.</p> <p>Example: a mobile telecommunications operator provides a Services for voice and SMS. Voice telephony and SMS are Applications implemented by the mobile communications Network. SMS requires Services that are often provided by third parties for message storage.</p> <p>Example: the Owner of a Home who is running an Application locally to reduce electricity consumption enters into an agreement with the electricity supplier to use the supplier's energy management Service to optimise use of electricity in combination with pricing offered by the supplier.</p>

<b>Service Agreement</b>	<p>Contract(s) between a Service Provider and the customer (end user, subscriber, consumer). The service agreement may be backed up by subordinate service agreements for the whole Service Supply Chain.</p> <p>Note: the IFRS CWA does not define the requirements for enterprise interoperability between Service Providers in the chain.</p> <p>Example: a contract to supply electricity, gas, water and sewerage services to a home.</p>
<b>Service Application</b>	<p>A service application is a software entity/bundle that delivers some specific service(s) to an end user.</p> <p>Example: none.</p>
<b>Service Bundle</b>	<p>A set of services delivered through a common means therefore attracting synergistic benefits.</p> <p>Example: a collection of TV services delivered using a DVB application. It may be a combination of freeview and paid-for channels, sometime called a "bouquet".</p>
<b>Service bundles (OSGi)</b>	<p>Term used by OSGi to describe the set up and control of applications: An OSGi bundle is comprised of Java classes and other resources which together can provide functions to device owners and provide services and packages to other bundles.</p> <p>Example: none.</p>
<b>Service Level Agreement</b>	<p>A formal agreement between a Service Provider and customers to provide a certain level of service. Penalty clauses might apply if the SLA is not met.</p> <p>Example: a broadband service is offered with a SLA that guarantees 8 Mbps downlink and 2 Mbps uplink with 99.999% availability.</p>
<b>Service levels</b>	<p>Parameters of a service as delivered to an end user by a service provider.</p> <p>Example: the data-rates and availability given above.</p>
<b>Service Provider</b>	<p>Any organisation or entity that provides any good or service to a consumer.</p> <p>Example: a telecommunications operator; a supplier of gas.</p>
<b>Service Supply Chain</b>	<p>The entities that are necessary to deliver the service form a service-supply chain.</p> <p>Example: The Application Home Initiative has identified 11 such entities that span the creator of the service, the service aggregator, service provider, service operator, network operator, service distributor, subscriber and the end user. The European Application Home Alliance has further subdivided the end user entity into customer and consumer. Each Entity must have an overall contractual relationship with the service provider and will have back to back contracts with the adjacent entity in the service supply chain. These contracts will each ensure that the Service level requirements of the service are fulfilled and that each entity obtains a benefit from the service supply.</p>
<b>Subscriber</b>	<p>A person or organisation who contracts with a provider to use a service on a subscription (regular and renewed payment) basis. A subscriber may be the consumer or the subscription may be provided by organisations such as social service or healthcare provider.</p> <p>Example: a Consumer who has a Service Agreement with a provider of TV services.</p>
<b>System</b>	<p>A group of independent but interrelated elements comprising a unified whole; A collection of components organized to accomplish a specific function or set of functions. [IEEE STD 610.12]</p> <p>System (process operation, function or activity) is an arrangement, a set, or a collection of concepts, parts, activities and/or people that are connected or interrelated to achieve objectives and goals. (This definition applies to both manual and automated systems). A system may also be a collection of subsystems operating together for a common objective or goal.</p> <p>A collection of application instances and service instances</p> <p>Example: a security system providing control of access to premises based on smart ID cards.</p>
<b>User</b>	<p>An entity that has the capability to originate, or respond to, events.</p> <p>Example: a human being, an application .</p>

## 131 3.1.2 Security

132

<b>Access rights</b>	<p>Permission and ability to use an object for a specified purpose – requesting information from it, changing values of variables in it or modifying its state.</p> <p>Example: read access to a shared variable; permission to turn on, or off, i.e. execute certain operations.</p> <p>Note: where more than one service or application requires access to an object for one or more specific purposes, then levels of access must be defined, including the definition of the primary owner of the access rights (possibly the owner of the object)</p>
<b>Authentication</b>	<p>The validation of a claimed identity.</p> <p>Example: The validation of a claimed identity of a user can be made by verifying some secret knowledge, key, or property associated with that user, e.g. a password, a SSL key, a PGP private key, or a hand-written signature.</p>
<b>Authorisation</b>	<p>The decision to permit a user to make none (deny access), one or more types (permit access) of operations on an object.</p> <p>Example: The permission is made by comparing the validated user's access rights with the user's requested action(s) on an object, for example to read and to modify some content of an object.</p>
<b>Security</b>	<p>Rules and policies stated by owners that control the use of their property by other owners.</p> <p>Example: people allocated car-parking spaces are allowed to open the garage doors. People with no allocation may not open the doors.</p>
<b>Physical Security</b>	<p>Rules and systems put in place to safeguard the Physical Access to a premise or devices from physical interference.</p> <p>Example: a self-opening and closing door for wheelchair access, compliant with standards for such devices.</p>
<b>Information Security</b>	<p>Information Security provides confidentiality, integrity, availability and accountability of data.</p> <p>Example: key for encryption or detection of tampering, access permissions for reading and writing objects, audit trails for modifications to data.</p>
<b>Security Requirements</b>	<p>The purpose, objectives and success criteria applied to an Application or Service.</p> <p>Note: This CWA specifies Requirements for Security in relation to Levels of Interoperability that cover both Physical and Information Security and these must be combined with Safety and other considerations such as the permission and priority of access, discovery, configuration and management.</p> <p>Example: none.</p>

133

134

135

136

137

138

139

140

141

142

143

144

## 3.1.3 Interaction Models

All methods or protocols that operate under particular specifications use models for the transmission of information and the configuration and managements of objects. The commonly used methods are listed below:

An interaction between two interacting application entities (device or object) consists of the complete set of messages accepted by the device or object and the synchronisation of the outcome for each interaction between the two communicating entities using these messages. The messages define the application-layer protocol by which devices and/or objects communicate over a binding. The method of synchronisation defines the interaction model

<b>Acknowledgement</b>	<p>An object may acknowledge a command with a simple &lt;Acknowledgement of Receipt&gt; or respond with the information that the command has been completed, that it was unable to complete the command with the reason and may return parameters of its changed configuration following the completion of the command.</p> <p>Example: a door-opener device acknowledges that it received an instruction open the door. It does not confirm that it acted upon the instruction.</p>
<b>Broadcast</b>	<p>One-to-all communication method; a single transmit operation is used to distribute information to all receiving entities in a system.</p> <p>Example: there is a fire, open all the doors!</p>

<p><b>Command / Response</b></p>	<p>In this interaction model one object (the controller) initiates an interaction by issuing a command (request) to another object at a known interface, and the other object (the server) executes it and notifies the initiator by a response. The response typically contains information of new state or failure reports if not able to carry out the command contained in the originating message.</p> <p>Note: there is an implication that the operation requested in the Command has actually been executed, by contrast with the Acknowledgement model above. In some protocols, both the Command and Response are acknowledged.</p> <p>Example: the door is now open; the door was locked and could not be opened.</p>
<p><b>Data Driven</b></p>	<p>An object monitors the information placed on its network and if information is received that it has been instructed (programmed) to respond to, it will reconfigure its parameters or carry out an action according to its programming. On completion of an action or parameter change, the object will make available to other objects on the network any change in its configuration.</p> <p>Note: the data-driven interaction may be implemented using Broadcast or Multicast distribution of messages. It is implicit that messages are not commands requested by one object upon another.</p> <p>Example: an electric kettle generates a message to inform other devices that it has boiled the water.</p>
<p><b>Distributed Shared memory</b></p>	<p>A distributed programming method that refers to making the individual application memory of individual devices/objects in a distributed home system to appear as a single address space. Local changes of content of memory locations are propagated through the system by a suitable communication protocol.</p> <p>Example: read the data at this location, write this data to that address. There is an expectation that something will happen, e.g. the location written to may be the actuator that opens the door; the location read from may contain the bits that say that the door is opening.</p>
<p><b>Event Driven</b></p>	<p>An object is said to use an event-driven interaction model when its state and operation is determined by events received at its input(s), and it notifies other objects of its (change of) status through the same method. This method is also known in some HES specifications as "data-driven". An event-driven communication model is able to respond better to real-time changes and stimuli than conventional request/reply mechanisms.</p> <p>Note: the event-driven interaction may be implemented using Broadcast or Multicast distribution of messages. It is implicit that events are not commands requested by one object upon another.</p> <p>Example: Everyone! Somebody opened the door!</p>
<p><b>Multicast</b></p>	<p>One-to-many communication method: a single transmit operation is used to distribute information to all registered or interested receiving entities in a system. E.g. an event multicast is an event that is sent to a subset of objects/devices in the system.</p> <p>Example: Security devices! Somebody opened a door!</p>
<p><b>ODP-RM</b></p>	<p>The Open Distributed Processing Reference Model specifies three kinds of interaction: asynchronous signals, flows or streams, and remote operations or remote procedure call. Both flows and operational interactions may be defined in terms of signals. For the purposes of this document we define here only the asynchronous signals, and operations/remote procedure call. Typically existing systems that target or relate to home electronic services use methods or protocols that refer to using some variant of an interaction model, often qualified by the implementation or communication method used to support the logic interaction model. The definitions for these commonly referred to variants are command/response and event-driven/shared variable.</p> <p>Example: none.</p>
<p><b>Shared Variable</b></p>	<p>A variant of the Distributed Shared Memory, in which individual variables in devices/objects in a distributed home system appear as a single local variable. Local changes of variable values are propagated through the distributed system by a suitable communication protocol. Also, an identifier in a network implemented using distributed shared memory mechanisms.</p> <p>Example: a interaction model used in ISO/IEC 14908.</p>
<p><b>Unacknowledged</b></p>	<p>An object may send a command to an other object and does not (expect to) receive a (tightly-coupled or any) reply.</p> <p>Example: open the door! I expect it to be open when I get to it.</p>

<b>Unicast</b>	<p>One-to-one communication method: a single transmit operation is used to send information to a single named receiving entity. E.g. an event unicast is an event that is sent to a specific, identified, object/device in the system.</p> <p>Note: command/response interactions are often implemented using unicast communications.</p> <p>Example: a comfort controller asks the kitchen sensor how for the temperature.</p>
----------------	---

145  
146  
147

### 3.1.4 Processes

<b>Application</b>	<p>Use of a technology, system, or product. An application may consist of a number of elements or entities working together to provide a service or product. It may utilise specific elements in a system or technology in delivering the application. Alternatively, an application may be a program that carries out a particular service within a computer, processor or (home) system.</p> <p>Example: see definition above.</p>
<b>Application programming interface</b>	<p>A defined set of calling conventions allowing a software application to access a particular set of services. An API consists of the routines, protocols and tools that programmers must use to ensure that their programs are compatible with the software that the API is defined for. A well defined API helps applications work together by providing the same basic tools for all programmers to use.</p> <p>Example: the TCP socket programming interface: open(), close (), listen(), accept(), select(), read(), write().</p>
<b>Configuration</b>	<p>The set of status parameters for an object or device.</p> <p>Example: a device is connected to the application using a certain network address, its objects are registered with objects in other devices.</p>
<b>Configuration Process</b>	<p>Configuration of parameters of an object or objects or applications. This may be carried out by means of a Configuration tool and other actions that may be automatic and driven by other services and/or applications.</p> <p>Example: the association of objects in a device with those in other devices.</p>
<b>Discovery</b>	<p>Enabling systems to discover new units and to recognise what they are. Objects may present or publish their parameters or respond to a broadcast for information about specific object types).</p> <p>Example: UPnP.</p>
<b>Discovery Process</b>	<p>The process of the above</p>
<b>Middleware</b>	<p>Middleware is a generic term for functions that make a communications infrastructure that is part of a distributed system usable by applications. Middleware may be used for the purposes of Interoperability to translate the data presented by an object under one specific home system specification to the requirements of another.</p> <p>Example: the IP routing functionality in a home gateway to ISP services provides middleware to connect with the ISP, register local devices for access to Internet services and route IP packets between local processes and external ones.</p> <p>Example: a smart meter provides middleware that authenticates application objects downloaded into it before allowing them to use its communications services to implement specific application functions.</p>

148  
149  
150  
151

### 3.1.4 Interoperability

<b>Coexistence</b>	<p>Objects and applications exist in the same environment but they do not conflict with one another but at the same time their functions are not related or dependent on one another.</p> <p>Example: a security service monitors events in a home via the smart electricity meter communicating via a Zigbee link to the home security gateway. Due to excessive traffic between other Zigbee connected devices, such as the Consumer Display Unit, the meter is temporarily too busy to relay security events and there is a delay in reporting a break-in.</p>
--------------------	---

<b>Interoperability</b>		<p>Interoperability is the ability of two or more networks, systems, devices, applications or components to exchange information between them and use (intelligently) the information so exchanged. (IEEE/CENELEC)</p> <p>The consistent use and identical measured effect of information exchanged between the services and devices comprising an application .</p> <p>Example: see elsewhere in this CWA.</p>	
<b>Interoperability Levels</b>		<p>For the purposes of this Interoperability Framework Specification, the levels of Interoperability describe the degree to which entities, systems, networks and devices are able to interwork together. Level of Zero describes the very basic interoperability of objects interworking within the same system environment. Each higher level increases the functionality and degree of Interoperability.</p>	
	<b>Current levels of Interoperability</b>	<b>Level 0</b>	Interoperability that occurs within a specific protocol or system (this may include applications that are specified and used within the system) and which may need to link to higher levels of interoperability in the same application domain
		<b>Level 1</b>	As level 0 + Interoperability that pertains between application domains
		<b>Level 2</b>	As level 1 + Interoperability that pertains between (a pair of different) specifications or protocols (1 : 1)
		<b>Level 3</b>	As Level 2 but between multiple (different) specifications or protocols (N : N)
	<b>Covered by IFRS</b>	<b>Level 4</b>	Manual installation and instantiation of applications under Level 3 including discovery, configuration and with any N:N system.
		<b>Level 5</b>	Automatic Installation of applications: as under Level 3
		<b>Level 6</b>	As Level 5 but including maintenance (upgradeability), diagnostics and security with the capability to remotely manage and secure any topology of systems, applications and objects
<b>Interworking</b>		<p>The capability to exchange information between services and devices of dissimilar capability and/or provenance such that interoperability is achieved.</p> <p>Example: a home gateway to ISP services provides interworking between Ethernet and Wifi media in the home and the ADSL media outside the home to support routing of IP packets so that the applications objects in the home are interoperable via IP protocol with application objects elsewhere.</p>	

152  
153  
154

**3.1.5 Objects**

<b>Address</b>	<p>A name that is used to locate an object for the purposes of communicating information.</p> <p>Example: a telephone number locates a specific phone line in the PSTN.</p>
<b>Application Object</b>	<p>A description of an application in terms of describing the action an application carries out. The "Application Object" carries a description of the action and of how it is identified, configured, managed and what its parameters are.</p> <p>Example: a shared variable that represents the temperature at a location defined by the name of the variable.</p>
<b>Device Object</b>	<p>A physical object or instance of a physical object.</p> <p>Example: a temperature sensor.</p>
<b>Functional Object</b>	<p>An object that carries out a particular identifiable application task.</p> <p>A collection of objects and actions on objects that models a particular identifiable application function within an application domain.</p> <p>Example: none.</p>
<b>Handle</b>	<p>A identifier with an assigned meaning in a specific context. A handle is often used with only temporary local meaning during the execution of an application to refer to permanent objects. It is often said to be "opaque", meaning it cannot be used except by the functions that understand how it was created, or "transparent", meaning that there is an agreed semantics that all can use.</p> <p>Example: when a shared object is opened, a handle is created by the local middleware that is communicated to remote objects that wish to use the shared object. All requests they make are with reference to the handle and they can never know where the object actually is.</p> <p>Example: the address in memory of a shared object is returned by the local middleware that is communicated to remote objects that wish to use the shared object. All requests they make are</p>

	with reference to the memory location and they can overwrite its contents as they wish.
<b>Name</b>	A handle that is used to identify an object to an application, possibly uniquely, possibly within a defined context or scope. It may be opaque or transparent according to application requirements.
<b>Object</b>	A discrete item that provides a description of anything in a system (Extracted from Google / Princeton.edu); a unit of software functionality (ISO 18012-2) : Generally an "Object" has an identity and parameters and may be configured or managed and these properties may be discovered. This definition of an object may therefore apply to any element of a system, it may be a wholly discrete entity or it may be a more complex object made up of a number of elements which act as one object and this may apply to applications and services as well as physical entities.  Example: none.
<b>Type</b>	A name that is used to identify the capabilities of an object for the purposes of an application.  Example: in C: typedef temperature double; i.e. a double-precision real number that represents a quantity denoted by temperature as understood by an application.

155

### Definitions

Where applicable these are numbered 3.1. Defined terms should be ordered alphabetically.  
The text could then read as follows:  
"For the purposes of the present document, the following terms and definitions apply:  
Definition1: explanatory text  
Etc"

156

157

158

159

### 3.2 Symbols (to be done)

#### Symbols

Where applicable these are numbered 3.1 (where there are no definitions) or 3.2.  
Suggested text is as follows:  
For the purposes of the present document, the following symbols apply:

<Symbol1>    <Explanation>  
<Symbol2>    <Explanation>

160

161

162

163

### 3.3 Abbreviations (to be done when document is nearly completed)

#### Abbreviations

Where applicable these are numbered 3.2 (where there are definitions but no symbols, or vice-versa) or 3.3.  
Abbreviations should be ordered alphabetically.

For the purposes of the present document, the following abbreviations apply:  
<ACRONYM1> <Explanation>  
<ACRONYM2> <Explanation>

An example is :  
CEN Comité Européen de Normalisation

164

165 **4. Conformance clauses**

166  
167 This Interoperability Framework Specification has the following requirements:

168  
169 **Identifier**

170 Any Object shall have a unique identifier  
171 See Clause 4.1.1 for detailed identifier requirements

172  
173 **Discovery**

174 Any system, specification or protocol that conforms to this standard shall have a means for enabling  
175 the discovery (of location and identity) of objects within the system by services or applications  
176 including those external to the system,  
177 See Clause 4.1.2 for detailed discovery requirements

178  
179 **Object Description**

180 Any Object that can be discovered under this standard shall (provided access rights allow) render up  
181 its specification, status and other necessary information to services or applications including those  
182 external to the system  
183 See Clause 4.1.3 for detailed object status requirements

184  
185 **Object Configuration**

186 Any Object that can be discovered (provided access rights allow) may be configured by services or  
187 applications including those external to the system or protocol within which they exist.  
188 See Clause 4.1.4 for detailed object configuration requirements

189  
190 **Object Management**

191 Any Object that can be discovered (provided access rights allow) may be managed by services or  
192 applications including those external to the system within which they exist.  
193 See Clause 4.1.4 for detailed object management requirements

194  
195 **Object Interaction Model**

196 Any specification or protocol in which an object can be referenced, shall ensure that information as  
197 to its interaction model may be made available, such that the service or application may interact with  
198 the object in a manner expected by the specification or protocol.  
199 The interaction model addresses the interactions between objects of the systems compliant with this  
200 framework for configuration, management, security and safety.  
201 See Clause 4.1.5 for detailed Object Interaction Model Requirements

202  
203 **Object Access and Safety Requirements**

204 Before any action is made by a service or application, it shall establish that it has permission to  
205 undertake the action. Permissions shall be assigned according to a specified hierarchy - this applies  
206 to all considerations of security and safety and is required to ensure that the locus of control of any  
207 object can be identified at any time.  
208 The security, safety and priority rules shall be enforced at object level and application model level.  
209 Under this standard, object operations and interactions shall be governed under these rules.  
210 However, operations and interactions within underlying standards will not be affected by these rules.  
211 See Clause 4.1.6 for Object Security, Access and Safety Requirements

212  
213 **4.1 Conformance sub-clauses**

214 **4.1.1 Identifier description and requirements**

215 It is a requirement of this specification that any object (device, equipment, system, application or  
216 service) shall be uniquely identifiable. This is to ensure that there can be no possible doubt as to  
217 which object is being addressed and where that object is. (This may not matter if the Interoperability  
218 level is lower than 6 since any device is unique within its environment but since ultimately all  
219 systems will be interoperable to level 6, this requirement has to apply to all objects)

- 220 ▪ Whether this is by means of a unique address or number or whether this may be derived from
- 221 non-unique addresses in relation to a uniquely identified environment (such as a house
- 222 address or specific network under a specific protocol in that house) is immaterial.
- 223 ▪ Handle – Any specific object may have as part of its unique identifier a set of characters or
- 224 bytes that provide information as to what the object is.

- 225       ▪ Number – Any object may have a unique number such that it (and only that specific object)
- 226       may be identified. This number may only need to be unique with relation to the network or
- 227       environment or subdomain in which the object is contained. This non unique number will
- 228       become unique when coupled with the address of the environment or network in which it is
- 229       contained. There are many number systems that result in unique numbers for identity such as
- 230       IPv6, RFID and so forth
- 231       ▪ Address – any environment will have an address or a unique identifier and this may be used in
- 232       conjunction with the unique identifiers of objects contained in subdomains, local networks or
- 233       environments to create a unique identifier.

234 See work on “Locators” (IRTF) - <http://www.irtf.org>

#### 235 236 **4.1.2 Discovery requirements**

237 The process and mechanisms used by a device or object to search, find/locate and acquire system

238 and application object handles and to realise its designed functionality to the end-user (being the

239 human or some other part of the system) is referred to as service discovery.

240 Support for discoverability is a fundamental requirement to ensure interoperability in loosely coupled

241 systems such as envisioned by this document (home electronic systems and services

242 environments), where devices and services will be installable professionally or by end users directly,

243 and where these devices and services will evolve in time. Existing systems that are not designed to

244 be solely installed professionally do specify protocols and mechanisms to allow the discovery of new

245 devices. This is often referred to as “service discovery”, and it consists of the set of mechanisms and

246 protocols that allow an object to announce or respond to queries related to its service by providing

247 information on its location (logical address or handle), what service it provides (what does it do?),

248 and how well does this service fit the query (how well does it do it? This may be available as

249 information that allows the quality of service of the object.)

250 Device (or object) discovery is driven by two scenarios: (i) new device/object installed in a system

251 and wants to offer its services (*registration/announcement*); (ii) new device/object installed in a

252 system and wants to use services from some other device(s)/object(s) (*discovery query*). In the

253 context of this document the basic requirements are to support interoperability are:

#### 254 **Object Interface Definition (Service and Attribute Naming)**

255 A common schema for service and attribute naming shall exist. The schema should support

256 placeholders for interface definition extensions to support manufacturer-dependent

257 enhancements (if any), as well as refined querying of the attributes.

#### 258 **Discovery initial communication method**

259 Devices or objects newly installed shall support both unicast and multicast messages on

260 their service discovery interface. Multicast addresses to be used must be publicly available,

261 preferably maintained by a suitable recognised (international) naming authority.

#### 262 **Discovery interaction model**

263 Devices and objects shall support both query (request-response) and announcement (event-

264 based) interaction models. This means that the devices will be able to respond to queries

265 about their services (scenario (ii) above), or can announce their presence at installation, or

266 periodically, according to their design.

#### 267 **Discovery-support infrastructure**

268 Devices and objects adhering to this standard shall operate in a decentralised (non-directory

269 based) discovery infrastructure. This means that devices and objects should not depend, nor

270 rely, on a single repository of registered active/available services to be registered with or to

271 acquire handles from in order to complete their discovery and configuration process.

#### 272 **Discovery scope**

273 Discovery scope refers to the topological (logical or network) extent of the service search.

274 Devices and objects adhering to this standard shall be able to configure and control the

275 discovery scope, independently of the discovery initial communication method being used by

276

277

278

279

280

281

282

283 any device or object in the system. The main reasons for this requirement are potential  
284 privacy and security considerations<sup>2</sup>and discovery interval duration.

285  
286 **Security**

287 See Access and safely discussion.

288  
289 **Discovery privacy**

290 See security and privacy discussion

291  
292 **4.1.3 Object Description requirements**

293 The categories of object status are based on different system aspects and concerns addressed by  
294 interoperability level. The higher interoperability level is the more items an object should include.

295 **Object Classification**

296 An object under this standard shall provide sufficient high-level abstract information to be  
297 classified for use by other objects, as well as enforcing security, safety and accessible rules.  
298 The minimum information should include: intended purpose, targeted application domain,  
299 and text description. It may include communication means, quality rating and quality  
300 guarantee. It is optional from level 3 downwards and mandated from level 4 upwards.

301  
302 **Object Functional Interface**

303 An object under this standard shall provide the functional interface description for other  
304 objects to access its internal status and invoke its actions. The description should provide  
305 the detail object access and invocation method. It should include a list of attributes and their  
306 read/write permission, and functions and their associated input and output parameters. It is  
307 optional from level 3 downwards and mandated from level 4 upwards.

308  
309 **Object Configuration Interface**

310 If an object under this standard is configurable if it can adjust its behaviour based on given  
311 attributes, the object shall provide the context interface description for configuration tools  
312 and/or other objects to access and modify its attributes. It should provide a list of  
313 configuration attributes and their corresponding read/write permission. It is optional from  
314 level 4 downwards and mandated from level 5 upwards.

315  
316 **Object Management Interface**

317 If an object under this standard is manageable, then the object shall provide management  
318 interface description for management tools and/or other objects to carry out the  
319 management tasks (e.g. diagnosis, trouble-shooting). It may provide supporting  
320 management type, a list of information and operation offered, and its associated interaction  
321 model. It is optional from level 5 downwards and mandated for level 6.

322  
323 **4.1.4 Object Configuration and Management Requirements**

324  
325 Object management requirements consider processes and mechanisms that are used for object life-  
326 cycle management, including installation, initialisation, termination, security, recovery and  
327 performance. The installation of a device or object is not enough; once installed a device/object will  
328 require information about the system it is installed in and other devices/objects that it can or should  
329 interact with to realise its functionality. It is assumed that an object is running on a fully operational  
330 network connection, which means all the necessary network configuration (network address  
331 assignment and interface initialisation) are completed successfully. The following items provide basic  
332 requirements to support interoperability for object management operations in the context of this  
333 document:

334  
335 **Independence from network configuration**

336 Object correct operation must not depend on network configuration information. For  
337 example, network addressees must not be used for object identification.

338  
339 **Installation**

---

<sup>2</sup> Note however that this is a very weak mechanism to address any privacy or security concerns in a home distributed system.

340 Objects can be installed in a variety of modes; they can come with a device, or can be  
341 installed remotely. Objects should be initialised to a correct and safe state. Once initialised  
342 they should make available their description and location as part of the discovery process.  
343

#### 344 **Initialisation**

345 Objects should be initialised to a correct and safe state. Once initialised they should make  
346 available their description and location as part of the discovery process.  
347

#### 348 **Discovery**

349 See Section 4.1.3: Discovery requirements.  
350

#### 351 **Configuration**

352 Objects should support a common defined interface for their configuration, if such actions  
353 are supported.  
354

#### 355 **Configuration methods**

356 A device or object falling under the scope and being compliant with the requirements of this  
357 document shall be able to complete their configuration with and without centralised  
358 configuration tool control or support. In either case, the device or object shall be able to  
359 indicate if it is auto-configurable or if it requires suitable configuration tools to be  
360 commissioned.  
361

#### 362 **Error management**

363 Objects should be initialised to a correct and safe state. Should an error occur, an object  
364 should provide a common interface to allow notification or detection of abnormal conditions  
365 such as an object unexpected failure, with the aim to recover in such way that it does not  
366 block other objects from continuing to participate in the application.  
367

#### 368 **Termination**

369 Wherever is supported, objects should provide common interface for safe and correct  
370 termination, which should include invoking processes to notify the new state to the rest of  
371 the system the object participates in.  
372

### 373 **4.1.5 Object Interaction Model Requirements**

#### 374 **Discovery Interaction Model**

375 The discovery interaction model addresses the interactions of system discovery operation  
376 aspect. The discovery interaction model ensuring objects under this standard should specify  
377 the discovery steps and messages during the discovery process. The basic interaction  
378 model is event-driven model. The command/response model could be used for the  
379 subsequent detail inquiry.  
380

#### 381 **Operation Interaction Model**

382 The operation interaction model addresses the interactions of system normal operation  
383 aspect. Mainly, the interactions involve two or several objects interaction to form an  
384 application process and achieve a certain task. It should be sufficient enough to enable  
385 typical application operations. The basic interaction model is event-driven model. The  
386 command/response model may be required for some applications.  
387

#### 388 **Configuration Interaction Model**

389 The configuration interaction model addresses the interactions of system configuration  
390 aspect. The interaction could be utilised by configuration tools and/or configuration objects  
391 under this standard to accomplish system configuration. The interaction model should  
392 acknowledge the configuration result to configuration command issuer(s) whether or not the  
393 corresponding configuration has been successfully carried out. Therefore, it should use the  
394 command/response model.  
395

#### 396 **Management Interaction Model**

397 The management interaction model addresses the interaction of system management  
398 aspect. The interaction could involve management tools and/or objects for management  
399 under this standard to accomplish system management functions. The interaction model  
400 should allow management functions to gather relevant information of object runtime and  
401

402 adjust object instance that is inappropriate for system for one that is appropriate. While the  
 403 event-driven model is appropriate for information gathering, the command/response model  
 404 may be required for object manipulation to ensure the operation reliability.  
 405

406 **Security Interaction Model**

407 The security interaction model specifies the interaction process to ensure the system wide  
 408 security within this standard framework. The security interaction model should be added on  
 409 top of operation interaction model for security aspect.  
 410

411 **Safety Interaction Model**

412 The safety interaction model is built on top of operation interaction model to address safety  
 413 concerns.  
 414

415 **Note:** Since under this framework any object may be configured or managed by multiple services or  
 416 applications, it is important that a hierarchy of management exists and configuration only occurs with  
 417 the permission of the senior service or application.  
 418

419 **4.1.6 Object Security and Access requirements**

420 Interoperability implies the interworking and co-operation of multiple devices, systems and networks  
 421 and as the level of interoperability reaches above level 3 and certainly by level 6 there are likely to  
 422 be new requirements on what an object can or cannot do, who or which system may have  
 423 permission to control it and consideration must be given to the aspects of safety for specific objects  
 424 systems and applications. It is evident that what may be both safe and secure within a closed  
 425 system may become unsafe or insecure if that same system is opened up to multiple other systems  
 426 by interoperability.  
 427  
 428

429 Security is the first casualty of an open distributed networked system. The passage of traffic from  
 430 originator to recipient(s) must pass certain tests before being forwarded or executed. Within a certain  
 431 scope no checks may be needed, e.g. when the system is entirely self-contained and cannot  
 432 communicate externally.  
 433

434 This may be seen according to the following table:

435 Table 1. Security, safety and Access Rights and their priority by Interoperability Level  
 436  
 437

Interoperability Level	Security	Safety	Priority	Access Rights
0	Within Application as appropriate	See note 1, local remote operation	N/A	Within Application as appropriate
1	Within Applications as appropriate	See note 1, local remote operation	Applications set priority for control	Within Applications as appropriate
2	Within Applications as appropriate	See note 1, local remote operation	Applications set priority for control	Within Applications as appropriate
3	Within Applications as appropriate	See note 1, local remote operation	Applications set priority for control	Within Applications as appropriate
4	Installer responsibility See note 2	Installer responsibility See note 3	Installer responsibility See note 3	Installer responsibility See note 3
5	Application design responsibility see note 4	Application design responsibility see note 5	Application design responsibility see note 5	Application design responsibility see note 5
6	As level 5 but with remote management see note 6	As level 5 but with remote management see note 7	As level 5 but with remote management see note 7	As level 5 but with remote management see note 7

438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498

Notes on Table 1.

1. It is important to recognise that there are many instances where automatic operation can result on unsafe conditions. Where these are similar to (say) the setting of controls on a (cooker) oven or washing machine or central heating boiler, then provided the automatic remote control does not set conditions that a person manually would not set up, the conditions are no more or less safe than a non automatic set up. However, when the setting up is physically remote, it is important to ensure that the conditions of the operation are safe when the operation takes place and have not changed since the conditions were inspected manually and set for automatic operation. Thus an oven may be set for remote operation with specific cooking cycle requested but if between the set up and the operation, the door is opened, the oven must be reset for automatic operation before the operation can take place.

2. Under this Framework at Interoperability Level 4 it is the Installer's responsibility to ensure that the configuration of the operation and the local management of applications is appropriate and protected by secure means. This may mean that the use of local password protection is necessary or that information flows are encrypted.

3. At this level of interoperability multiple applications may control any one device or object. It is the installer's responsibility to ensure that a device may be given specific access rights that relate to specific applications. For instance an object or device may carry out a life critical operation and also be part of an application that is important to another service. It is essential that there shall be a hierarchy of access, priority and control that prioritises life critical actions over mission critical actions over other important applications. It is also important to recognise that circumstances may change and therefore priorities of access will also change and that the installer must recognise this and be able to change these when new equipment, devices or objects are installed or new uses are made of them.

4. When systems are automatically configured when new devices, equipment or objects are installed or when new applications are implemented with new equipment or systems, the burden of configuration is suitably protected by secure means as appropriate.

5. As with note 3. there is a responsibility for ensuring the safety through access control and understanding the priority of specific equipment and devices. Whereas under note 3 this is the responsibility of the installer, when applications are set up automatically, the application itself shall determine its priority to have access and control specific equipment, objects or devices. For instance an energy management application may control the temperature in a room to ensure the most efficient use of energy but it would be overridden by a life support system whose task was to ensure a patient was kept at a particular level of comfort.

6. As with note 4 there is a need to secure specific operations as appropriate. However, with control and operation remote from the house the whole communication chain must have a level of security that is appropriate to the application being controlled. Since any application could be subverted by an insecure communication link, this may mean at Interoperability level 6 all communication must be both reliable and secure for home control, security and life critical applications.

7. As with note 5, priority, safety and access control are highly important but in addition to the application having control, this control may be proxied to remote systems that may use intelligent means to set priorities. They may also set up new applications and it will be necessary for the remote system to be able to interrogate applications and devices to determine their settings, attributes and parameters and be able to reset safely the hierarchy of access rights, priorities in order to maintain the maximum level of safety. It is appreciated that this is difficult to achieve, but it is however, very important to ensure any modification of an existing system is fully considered and thought through even by autonomous systems.

499 **Annex A Informative Annexes**

500 **A.1 Use Cases**

501 **A.1.1 Methodology**

502 The use cases listed at this section is used as the base to develop this standard. They also serve as  
 503 test case to validate the design. These cases try to illustrate the generic problems rather than  
 504 exhaust all possibilities.  
 505

506 It should be noted that having developed an appropriate methodology to create use cases, the  
 507 various TAHI Industry Sector Groups as well as industry attending the CWA will be encouraged to  
 508 submit scenarios that may be built into use cases for demonstration purposes in this Annex.  
 509

510 Describe Scenario – assumptions about the overall nature of the environment in which the  
 511 system operates;

- 512 ■ eg someone/something  
 513 (is doing .....)  
 514 (needs to know ....) and  
 515 needs (to have the following information .....)  
 516 (control the following .....  
 517 and will need to use the following resources  
 518 (Object 1, Object 2, .. Object n – 1, Object n)  
 519 in the following manner (set of methods . . . )  
 520

521 Describe use-case:

522  
 523 The use case is a common technique to capture the required system behaviours and  
 524 requirements requested by the stakeholders. The use case is a hub to scaffold various aspects  
 525 of system requirements. Since interoperability is only one aspect in system requirements, the  
 526 interoperability requirements are normal buried within operation processes. However, the  
 527 interoperability is the key focus of this framework, the interoperability requirements should be  
 528 highlighted and the major parts of normal use case detail only provide the context and  
 529 background to comprehend the interoperability related requirements. To achieve this, the five  
 530 W's and one H approach has been adopted to extract the interoperability concerns and avoid  
 531 the unnecessary details of the rest. While the five Ws are who, what, where, when and why, and  
 532 one H is how. When the use cases record interoperable requirements for a piece of system, the  
 533 cases under consideration should focus on the interactions between IFI framework and other  
 534 system components since the IFI framework responds to handle interoperability issues in  
 535 systematic manner. The approach can be outlined as the following table. Five Ws should be  
 536 provided by industry contributor and one H is mainly responsible by project team. The priority is  
 537 the decision made by project team and steering group. While five Ws are the main content of  
 538 use case, one H and priority is derived from the use case content for design and analysis  
 539 purpose that is not considered as use case.  
 540

<b>Who</b>	It states the primary stakeholder, who initiates the interactions with system, especially with IFI framework. The primary stakeholder can be system components (e.g. sensor, actuator) and system users (e.g. end user, installers, and maintenance engineer). The statement of primary stakeholder implies the intention and its perspective.
<b>What</b>	Similar to the normal use case description, it provides the step-by-step interaction details to extract what the requirements are. Rather than recording the operation process detail, it provides the context of interoperable action and identifies the involvement of interoperation.
<b>Why</b>	It underpins and justifies the interoperable challenges described by the case. It is also desirable to state its necessary and importance.
<b>Where</b>	It outlines the place where the interoperations occur.
<b>When</b>	It states the phase during the system lifecycle: installation, commission, operation, maintenance and upgrade.
<b>How</b>	It provides conceptual solutions requesting the IFI framework to achieve.
<b>Priority</b>	It relates the case to the interoperability level and will be given priority in term of IFI framework design and development.

541  
542  
543  
544  
545

The following content is an example to illustrate how to use the table to document a use case. The use case is to use a movement detection sensor to control a light on/off. When the sensor detects occupancy, the light is on; otherwise, the light is off.

<b>Who</b>	Movement detection sensor (system integration)
<b>What</b>	1. Movement detection sensor detects movement. 2. The sensor informs a light switch. 3. The light switch switches the light.
<b>Why</b>	1. Movement detection sensor and light switch use different home network technology. 2. Movement detection sensor exists at high security network and light switch exists at low security network.
<b>Where</b>	The movement information transfers from sensor to light switch
<b>When</b>	Operation phase
<b>How</b>	1. Transform the sensor network format to the light switch network format. 2. Align the security level between sensor and light switch.
<b>Priority</b>	Interoperability level 2-3 and priority high

546  
547  
548  
549  
550  
551  
552

## A.1.2 Scenarios

The scenarios are the 7 Interoperability Levels. We assume that any of the security levels could be applied to any of these interoperability levels. The safety levels are properties of any use-case that must be proved to apply.

Operational Interoperability	<b>Level 0</b>	Interoperability that occurs within a specific protocol or system (this may include applications that are specified and used within the system) and which may need to link to higher levels of interoperability in the same application domain
	<b>Level 1</b>	As level 0 + Interoperability that pertains between application domains
	<b>Level 2</b>	As level 1 + Interoperability that pertains between (a pair of different) specifications or protocols (1 : 1)
	<b>Level 3</b>	As Level 2 but between multiple (different) specifications or protocols (N : N)
Configuration Interoperability	<b>Level 4</b>	Manual installation and instantiation of applications under Level 3 including discovery, configuration and with any N:N system.
	<b>Level 5</b>	Automatic Installation of applications: as under Level 3
	<b>Level 6</b>	As Level 5 but including maintenance, diagnostics and security with the capability to remotely manage and secure any topology of systems, applications and objects

553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567

### A.1.2.1 Level 0

A consumer, Mr. X, a first time buyer, buys a flat in a new-build block of apartments. Each flat is equipped with the following systems: security (from company A); smart metering with consumer display for gas and electricity (from company B), that has the optional capability (also from company B) to manage appliances in the flat; and comfort control for heating, (from company C). Company A offers the security product as a service that Mr X can subscribe to through the building management company. The smart metering system is an early product available from company B that is certified to comply with the CEN/CENELEC requirements for interoperability of smart meters and consumer displays. The appliances were supplied by company D and implement the International Standard (IS) P. The comfort control system, also from company D, implements IS Q.

All the above products are standalone and use system specific communications media: hardwired detectors and a second telephone line for the security system; the PLC for the smart meter, with short-range wireless

## CWA XXX-1:200X (E)

568 to the consumer display and a mixture of PLC and wireless to appliances; and proprietary wired media for  
569 the comfort control system.

570  
571 Mr X is happy to accept these systems due to a discount from the developer of the apartment block.

572  
573 Lesson: there is no problem until Mr. X creates one, and he is about to do just that.

### 574 575 **A.1.2.2 Level 1**

576  
577 Mr. X likes his individual systems but is mystified that comfort control is separate from appliance  
578 management. He would like his comfort control system to work with the smart meter system and save him  
579 more energy. The salesman from company D explains that his engineers plan to develop products that  
580 provide adaptation between P and Q, but that company B does not supply any comfort control application.  
581 However, company D can supply a separate management system that does manage all devices, P or Q, but  
582 it does not communicate with the meter or the CDU, requiring a separate console or a PC, USB interface to  
583 P or Q, and special application.

584  
585 Lesson: Mr. X has entered into more of a commitment than he imagined by accepting the vendor's packaged  
586 up systems. The gateways and adaptors add complexity.

### 587 588 **A.1.2.3 Level 2**

589  
590 Mr. X decides to change his energy supplier to company E, that offers the option to communicate with  
591 appliances using IS Q. The consumer display has to be exchanged because the wireless technology is  
592 different, although there are numerous products from companies F, G and H that offer protocol translation  
593 and adaptation, Neither company B nor company E guarantee that these gateway products will work.  
594 Company E warrants that devices implement Q (the comfort control system) can be managed using its  
595 approved consumer displays and recommends a gateway product from company I that can adapt P and Q to  
596 allow communication with the appliances. However company B does not make any claim that the appliances  
597 will work with company E's products and cancels the optional agreement with Mr. X to manage the  
598 appliances.

599  
600 Through a change in supplier, Mr. X has gained integrated energy and comfort control management but has  
601 lost the capability to manage other appliances unless he buys the gateway, even though this will not help  
602 him unless he can replace company D's management product. He has a redundant consumer display unit.  
603 Also, he bought a new thermostat, made by company L, that claims compliance to the same specifications  
604 as some of his other devices. Unfortunately, it cannot be used by the energy management system because  
605 company L uses a correct but incompatible variation of the security protocol, even though this is an IS.

606  
607 Lesson: more gateways *and* loss of functionality. More options appear as devices get more diverse.

### 608 609 **A.1.2.4 Level 3**

610  
611 Mr. X falls in love and gets married. Mrs. X moves into the flat and brings with her an entertainment system  
612 that uses IS R. The manufacturer, J, of R compatible products supplies a product (a set-top box plugin with  
613 wireless, PLC and Ethernet capability) that can communicate with products implementing P and Q, and the  
614 X's can now detect that they have access to all their consumer appliances and systems via their TV set.  
615 They cannot use the management applications that they used previously (which came from other vendors)  
616 but they can adjust parameters manually.

617  
618 Stop press: Mrs. X's aged parents have recently become unable to continue to live independently and want  
619 to move in with the X's. They need to move to a larger premises. With the P-Q-R gateway from company J,  
620 they can now take all their appliances from the flat and continue to use them in the new home. The senior  
621 residents often use the TV to communicate with their GP, which required a change of broadband supplier,  
622 and it is promising that there are products implementing P that also provide health care sensing. However,  
623 the security requirements arising from the external connection are far in excess of the features implemented  
624 by other P products, which cease to function when the parents system is running.

625  
626 Lesson: better gateways and restoration of some functions. Incompatibility at higher layers of more complex  
627 function combinations.

### 628 629 **A.1.2.5 Level 4**

630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690

Company J enhances its gateway product to accommodate the lower security capabilities of some products. A side-effect is that the TV can now be the smart metering CDU, although the energy supplier, while welcoming increased connectivity, is less confident about the possible security issues. Unfortunately the set-top box power-supply is now overloaded and the device fails frequently, losing all functionality. However, mass replacement of set top boxes is already underway for the latest upgrade to digital TV, so this is smoothed over. Too late – consumers lose confidence in that product and an opportunity opens for equivalent adaptation functions that could live in the meter, or the broadband gateway, or an entirely separate but equivalently connected device.

Company J sells its gateway capability to meter and home gateway vendors and the market expands rapidly. However, many operations are manual, especially configuration for different applications, even though discovery is automated, but just within the single home. J corrects this rapidly and offers the X's the facility, via its web pages to download applications compatible with its gateways and with devices and services from A, B, C, D, etc.

Meanwhile, consumers have forgotten that P, Q and R exist. In fact, they have converged, and the role of J's gateway is to manage applications and devices – discover what is in the vicinity, configure it to execute the applications to which the consumer has subscribed.

Lesson: the gateway element is critical, even if there are fewer instances. The evolution of protocols means that its role has changed.

#### **A.1.2.6 Level 5**

Exploiting external connectivity, third party service providers compete and collaborate with the X's energy, comms and healthcare companies to offer outsourcing of application functions.

Compatibility of in-home protocols with external communications services in compliance with International Standards allows a decentralisation of functions. Company J goes entirely virtual with a massive solar-powered datacenter in the Sahara offering customized services and applications, downloaded and managed via key interconnection functions, usually in a consumer's main gateway into his preferred supplier of Internet services (DSL, WiMAX, HSPA, PLC, etc.).

In spite of this capability, installers and service engineers from a range of providers continually visit the X's to investigate unexpected behaviours, especially after Mr. X has downloaded a new module and installed it himself. Because the devices and external services in his installation are Level 5 interoperable, these modules are able to install themselves automatically and function to a certain extent.

Lesson: unless an installation has the capability to link with external management for diagnostic purposes and to control installation expansions and consumer-installed upgrades, the necessary control over a system cannot be maintained.

#### **A.1.2.7 Level 6**

Company J implements additional functionality in its discovery and configuration processes so that only known compatible revisions of Level 5 compliant products can seek out and associate their functions with devices in the X's system and services offered by J. It does this partly by implementing stricter policies for these processes that match product codes, serial numbers and revisions of hardware or software to a database of matching configurations, and partly through better communication with Mr. X through Web services so that he is aware of potential problems and issues.

### **A.1.3 IFRS Methodology**

#### **A.1.3.1 Working Assumptions**

- The collection and categorisation of information that supports a conformance claim and allows it to be tested in an appropriate setting is provided for within the standardisation process, for example via the PICS and PIXIT proforma model. This model should be used;
- A data model that captures object specifications and relationships is not a priority for the IFRS CWA stage of the standardisation process. Ultimately one may be required, and a language will be selected

- 691 for expressing it. It is desirable that this is compatible with the language and methodology in which  
 692 scenarios and use-cases will be captured;
- 693 • PICS and PIXIT proformas may be needed wherever issues of interoperability arise. Following further  
 694 study, some issues may be deemed to be interworking requirements as distinguished above.
  - 695 • Topics to be covered by the PICS and PIXIT include: PHY (pathway, plug/socket, media); Link (MAC,  
 696 DLC, including layer 2 forwarding); Network (sub-network and device addressing, distribution mode);  
 697 Transport (end-to-end delivery and end-point addressing); Session (discovery, configuration and  
 698 platform-specific protocols); Presentation (abstract and concrete syntax of message structure);  
 699 Application (object specification and interaction protocols). It is recognised that these terms may not be  
 700 compatible with terms used in other specification approaches;
  - 701 • Specific HBES technology platforms may already have equivalent conformance proformas for all, some  
 702 or none of these layers (e.g. where reference is made to existing standardised conformance  
 703 specifications);
  - 704 • Furthermore, there are several platforms with interoperability guidelines that are well-established, and  
 705 standardised by CENELEC, CEN and ETSI. These provide a basis on which to build the proformas to be  
 706 included in the IFRS Agreement;
  - 707 • Security in such cross-platform, mixed location systems is a key issue and the source of many  
 708 interoperability failures and vulnerabilities. Some terminology may need further examination. The focus  
 709 will be on requirements and conformance, not solutions.

710  
 711 **A.1.3.2 Information to be Supplied**  
 712

Step/Function	Discovery	Configuration	Operations	System Management
Processes	Outlines the methods associated with the discovery of an object in the specific system.	Outlines the methods used to configuring an object or application object in the specific system.	Outlines the action of how applications are instantiated and operate in the specific system.	Outlines how an object or set of objects may be managed within the specific system.
	Discovery			
Security	The level of security provided solely by the specific system in the action of discovery.	The level of security provided solely by the specific system in the action of configuration.	The level of security provided by any application provided under the specific system.	The level of security provided solely by the specific system in the action of management.
		Object access and safety requirements		
Enablers	The methods used by the specific system to execute discovery.	The methods used by the specific system to execute configuration.	The methods used by the specific system to define and create applications and application models.	The methods used by the specific system to execute management.
	Identifier Object description	Object configuration		Object Management
Interaction Model	The methods used by the specific system to provide interaction between objects and other objects in the process of discovery.	The methods used by the specific system to provide interaction between objects and other objects in the process of configuration.		The methods used by the specific system to provide interaction between objects and other objects in the process of management.
			Object Interaction Model	
Cross Standard Support	Records ny standard, system, sub-system or protocol that has been identified as having a specific interface between it and another protocol, such translations or APIs are often created by a specific protocol and flow from it or to it,			

713  
 714 For each column, a product may comply with IFRS at any level between 0 and 6.  
 715

716 **A.1.3.3 Architectural Issues**  
 717

718 It is implicit that there will be a function that is able to match between systems, media and protocols for  
 719 products offering interoperability at Level 3 and above. Such functions already exist in a variety of forms from  
 720 Level 0 upwards:

- 721
- 722 • A device supporting 2 interfaces to separate media implementing a single HBES specification. The  
 723 device implements interworking at link level, receiving a message on one link and retransmitting it on the  
 724 other without change to the contents. Interoperability issues remain between the functions implemented  
 725 in interacting devices attached to the media;
  - 726 • A device supporting 3 or more interfaces to separate media implementing a single HBES specification.  
 727 The device is a router and must observe the routing protocol of the specification. Other interoperability  
 728 considerations are as noted above;
  - 729 • A device implementing one media interface to a single HBES specification and a second interface to  
 730 another system. This is commonplace with devices that connect to the Internet through a home gateway,  
 731 using IP as a bridging protocol;
  - 732 • To be completed.

733  
 734 Arial 10 is a good choice of font for plain text. Following this recommended font and font size will in the long  
 735 run ensure a common look and feel to all CWAs.

#### User Defined clauses and subclauses

The chapters below will contain some further elements to be kept in mind if one wants to comply with the PNE-rules. For the sake of example, these elements have been written as if they would be part of a CWA. **(Please be reminded that the rule of thumb for CWAs is that a CWA shall not unnecessarily deviate from the PNE-rules)**

736  
 737  
 738  
 739  
 740  
 741  
 742  
 743

## 4.2 Keep in mind: on numbering

### 4.2.1 Names/numbers of divisions and subdivisions

**Table 1 - Names of divisions and subdivisions**

English term	French term	Example of numbering
Part	partie	9999-1
Clause	article	1
Subclause	paragraphe	1.1
Subclause	paragraphe	1.1.1
Paragraph	alinéa	[no number]
Annex	annexe	a

744  
 745  
 746  
 747  
 748

### 4.2.2 Description and Numbering of divisions and subdivisions

#### Description and numbering of divisions and subdivisions

A subclause is a numbered subdivision of a clause. A primary subclause (e.g. 5.1, 5.2, etc.) may be subdivided into secondary subclauses (e.g. 5.1.1, 5.2.1, etc.).

A subclause shall not be created unless there is at least one further subclause at the same level. For example, a piece of text in clause 10 shall not be designated subclause "10.1" unless there is also a subclause "10.2".

749  
 750  
 751  
 752  
 753

## Figures

#### Figures

Figures shall be numbered with arabic numerals, beginning with 1. This numbering shall be independent of the numbering of the clauses and of any tables. A single figure shall be designated "Figure 1".

754

755  
756

**4.2.3 Text between headers**

**Text between headers**

There should be no text between two headers of a "different ranking". For example, the following is not allowed:

X.Y Header  
Text  
X.Y.1 Header

757  
758  
759  
760

**4.3 Keep in mind: on the Table of Contents**

**Table of Contents**

The table of content is an optional preliminary element, but is necessary if it makes the standard easier to consult. The table of contents shall be entitled "Contents" and shall list clauses and, if appropriate, subclauses with titles, annexes together with their status in parentheses, the bibliography; index(es); figures; tables. All the elements listed shall be cited with their full titles. Terms in the "Definitions, symbols and abbreviations" clause shall not be listed in the table of contents.

**In electronic documents, the table of contents shall be generated automatically and not set manually**

761  
762  
763  
764

**4.4 Keep in mind: on Annexes**

**Annexes**

There may exist Normative as well as Informative Annexes!  
Annexes shall appear in the order in which they are cited in the text. Each annex shall be designated by a heading comprising the word "Annex" followed by a capital letter designating its serial order, beginning with "A"; e.g. "Annex A". The annex heading shall be followed by the indication "(normative)" or "(informative)", and by the title, each on a separate line. Numbers given to the clauses, subclauses, tables, figures and mathematical formulae of an annex shall be preceded by the letter designating that annex followed by a full-stop. The numbering shall start afresh with each annex. A single annex shall be designated "Annex A". Informative annexes give additional information intended to assist the understanding or use of the standard and shall not contain provisions to which it is necessary to conform in order to be able to claim compliance with the standard. Their presence is optional. An annex's informative status (as opposed to normative) shall be made clear by the way in which it is referred to in the text, by a statement to this effect in the foreword and by an indication in the table of contents and under the heading of the annex.

Normative Annexes, see above!

**A bibliography, if present, shall appear after the last annex.**

765  
766  
767  
768

**4.5 Keep in mind: on Footnotes**

**Footnotes**

Footnotes to the text give additional information; their use shall be kept to a minimum. They shall not contain requirements. Footnotes to figures and tables follow different rules (see 6.6.4.9 and 6.6.5.7 of the PNE-rules). Footnotes to the text shall be placed at the foot of the relevant page and be separated from the text by a short thin horizontal line on the left of the page. An example is given for the footnote in the "Normative References" section

Footnotes to the text shall normally be distinguished by arabic numerals, beginning with 1, followed by one parenthesis and forming a continuous numerical sequence throughout the document: 1), 2), 3), etc. The

footnotes shall be referred to in the text by inserting the same numerals, as superscripts, after the word or sentence in question 1) 2) 3) etc.

There exists also notes within the text. They follow the example given in the section on the Scope:

[indent, separate paragraph]

**Notes are numbered (numbering restarts for each clause or subclause) if there is more than one Note in a clause or subclause. Notes shall be used for the purpose of giving additional information only and shall not contain provisions to which conformity is requested. Please use capitals when writing NOTE.**

#### **4.6 Keep in mind: on referencing inside the CWA**

##### **Referencing inside the CWA**

Use for example the following forms

- "in accordance with clause 3";
- "according to 3.1";
- "as specified in 3.1b);
- "details as given in 3.1.1";
- "see annex B";
- "the requirements given in B.2";
- "see the note in Table 2";
- see example 2 in 6.6.3";

It is unnecessary to use the term "subclause"

769  
770

771

---

772 **Annex B (Normative) : Interoperability Implementation Conformance**  
773 **Statement Proforma**  
774

775 **B.1 Scope**

776 This document provides the Interoperability Implementation Conformance Statement (IICS) proforma for the  
777 Conformance Clauses in the IFRS specification.  
778

779 The present document details in tabular form the implementation options, i.e. the optional functions  
780 additional to those which are mandatory to implement.  
781

782 **B.2 References**

783 The following documents contain provisions which, through reference in this text, constitute provisions of the  
784 present document. References are either specific (identified by date of publication, edition number, version  
785 number, etc.) or non-specific;  
786

- 787
- 788 • For a specific reference, subsequent revisions do not apply;
  - 789 • For a non-specific reference, the latest version applies.
- 790 1. ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile,  
791 conformance testing specifications; Standardization methodology".
  - 792 2. ISO/IEC 9646-1: "Information technology - Open Systems Interconnection - Conformance testing  
793 methodology and framework - Part 1: General concepts".
  - 794 3. ISO/IEC 9646-7: "Information technology - Open Systems Interconnection - Conformance testing  
795 methodology and framework - Part 7: Implementation Conformance Statements".

796 **B.3 Definitions and abbreviations**

797 **B.3.1 Definitions**

798 For the purposes of the present document, the terms and definitions given in TS 101 761-2 [1], ISO/IEC  
799 9646-1 [3], ISO/IEC 9646-7 [4] and the following apply:  
800

801 **Implementation Conformance Statement (ICS):** statement made by the supplier of an implementation or  
802 system claimed to conform to a given specification, stating which capabilities have been implemented.

803 NOTE: The ICS can take several forms: protocol ICS, profile ICS, profile specific ICS, information object ICS,  
804 etc.  
805

806 **ICS proforma:** document, in the form of a questionnaire, which when completed for an implementation or  
807 system becomes an ICS.  
808

809 **Protocol ICS (PICS):** ICS for an implementation or system claimed to conform to a given protocol  
810 specification.  
811

812 **Interoperability ICS (PICS):** ICS for an implementation or system claimed to conform to a the IFRS  
813 requirements.  
814

815 **B.4 Requirements for Conformance to this IICS**

816 To be added.  
817

818 **B.5 Instructions for Completion of the IICS**

819 To be added  
820

821 **B.6 Global Statement of IICS Conformance**

822 Complete the Table below as follows:

823 Y = full compliance, all requirements of the applicable IFRS conformance clause are observed;

824 P = partial compliance, some requirements are complied with others are not;

825 N = no compliance, none of the requirements are complied with.

Conformance Clause	Level 3	Level 4	Level 5	Level 6
Discovery Process				
Discovery Security				
Discovery Enablers				
Discovery IM				
Config Process				
Config Security				
Etc.				

826

827 **Bibliography**

828 (The bibliography is optional)

829

830 The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

831

832 - &lt;Publication&gt;: "&lt;Title&gt;".

833

834