



DPC: 24 / 30484383 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 29 January 2024

Origin: International

Latest date for receipt of comments: 20 March 2024

Project No. 2023/02963

Responsible committee: GEL/65/5 Devices and integration in enterprise systems

Interested committees:

Title: BS EN IEC 62541-21 OPC Unified Architecture

Part 21: Device Onboarding

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 20 March 2024**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: Ms Charmaine Mukherjee (BSI)

Direct tel:

E-mail: charmaine.mukherjee@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER:

IEC 62541-21 ED1

DATE OF CIRCULATION:

2024-01-26

CLOSING DATE FOR VOTING:

2024-04-19

SUPERSEDES DOCUMENTS:

65E/956/NP, 65E/1016/RVN

IEC SC 65E : DEVICES AND INTEGRATION IN ENTERPRISE SYSTEMS

SECRETARIAT:

United States of America

SECRETARY:

Mr Donald (Bob) Lattimer

OF INTEREST TO THE FOLLOWING COMMITTEES:

PROPOSED HORIZONTAL STANDARD:



Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.

FUNCTIONS CONCERNED:

☐ EMC

☐ ENVIRONMENT

☐ QUALITY ASSURANCE

☐ SAFETY

☒ SUBMITTED FOR CENELEC PARALLEL VOTING

☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

Attention IEC-CENELEC parallel voting

The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting.

The CENELEC members are invited to vote through the CENELEC online voting system.

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

OPC Unified Architecture – Part 21: Device Onboarding

PROPOSED STABILITY DATE: 2026

NOTE FROM TC/SC OFFICERS:

Copyright © 2024 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

CONTENTS

Page

1	FIGURES	iii
2	TABLES	iv
3	1 Scope	1
4	2 Normative references	1
5	3 Terms, definitions, and conventions	2
6	3.1 Terms and definitions	2
7	3.2 Abbreviations and symbols	4
8	4 Onboarding Model	5
9	4.1 Device Lifecycle	5
10	4.2 Concepts	7
11	4.2.1 Secure Elements	7
12	4.2.2 Firmware and Applications	7
13	4.2.3 Transfer of Physical Control	8
14	4.2.4 Trust on First Use (TOFU)	8
15	4.2.5 SoftwareUpdateManager	9
16	4.2.6 Roles and Privileges	9
17	4.3 Device Workflows	10
18	4.3.1 Distribution	10
19	4.3.2 Onboarding	10
20	4.3.3 Application Setup	10
21	4.3.4 Configuration	10
22	4.3.5 Operation	10
23	4.3.6 Decommissioning	11
24	5 Identities	11
25	5.1 Overview	11
26	5.2 Device Identity	11
27	5.3 ProductInstanceUri	12
28	5.4 Composite Identity	12
29	6 Ticket Semantics	13
30	6.1 Tickets	13
31	6.2 Ticket Distribution	14
32	6.3 Authentication	14
33	6.4 Acquiring and Validating Tickets	15
34	7 Device Authentication	16
35	7.1 Overview	16
36	7.2 Pull Management	18
37	7.3 Push Management	20
38	7.4 Alternate Authentication Models	21
39	8 Ticket Syntax	22
40	8.1 Signed Ticket Encoding	22
41	8.2 Ticket Types	23
42	8.2.1 EncodedTicket	23
43	8.2.2 BaseTicketType	24
44	8.2.3 DeviceIdentityTicketType	24
45	8.2.4 CompositeIdentityTicketType	25
46	8.2.5 TicketListType	25

49	8.2.6	CertificateAuthorityType	26
50	9	Information Model	26
51	9.1	Overview	26
52	9.2	Registrar	26
53	9.2.1	Overview	26
54	9.2.2	DeviceRegistrarType	27
55	9.2.3	ProviderIdentities	28
56	9.2.4	UpdateSoftwareStatus	29
57	9.2.5	RegisterDeviceEndpoint	29
58	9.2.6	GetManagers	30
59	9.2.7	ManagerDescription	31
60	9.2.8	RegisterManagedApplication	31
61	9.2.9	DeviceRegistrar	32
62	9.2.10	DeviceRegistrarAdminType	32
63	9.2.11	RegisterTickets	33
64	9.2.12	UnregisterTickets	33
65	9.2.13	DeviceRegistrationAuditEventType	34
66	9.2.14	DeviceIdentityAcceptedAuditEventType	34
67	9.2.15	DeviceSoftwareUpdatedAuditEventType	35
68	9.3	Device Configuration Application (DCA)	35
69	9.3.1	Overview	35
70	9.3.2	ProvisionableDevice	36
71	9.3.3	ProvisionableDeviceType	37
72	9.3.4	RequestTickets	37
73	9.3.5	SetRegistrarEndpoints	38
74	9.3.6	ApplicationConfigurationType	38
75	10	Namespaces	39
76	10.1	Namespace Metadata	39
77	10.2	Handling of OPC UA Namespaces	39
78	Annex A (normative)	Namespaces and Identifiers	41
79	A.1	Namespace and Identifiers for the Onboarding Information Model	41
80			
81			

FIGURES

82

83 Figure 1 – The Lifecycle of a Device..... 5

84 Figure 2 – Device Hardware and Software Layers 7

85 Figure 3 – Possible Transfers of Physical Control..... 8

86 Figure 3 – Relationship between Devices, Actors, Identifiers and Tickets 11

87 Figure 4 – Device Authentication using Pull Management..... 18

88 Figure 5 – Requesting Certificates using Pull Management 19

89 Figure 6 – Device Authentication using Push Management..... 20

90 Figure 7 – Updating Certificates using Push Management 21

91 Figure 8 – Alternate Authentication Models with Pull Management 22

92 Figure 9 – Registrar Address Space for Onboarding Workflow..... 27

93 Figure 10 – Device Address Space for Onboarding Workflows..... 36

94

95

TABLES

96		
97	Table 1 – The Actors in the Device Lifecycle	5
98	Table 2 – The Stages in the Device Lifecycle	6
99	Table 3 – Well-known Roles for Onboarding	9
100	Table 4 – Privileges for Onboarding	9
101	Table 5 – RFC 7515 Header Fields.....	23
102	Table 6 – EncodedTicket Definition	24
103	Table 7 – BaseTicketType Structure	24
104	Table 8 – BaseTicketType Definition	24
105	Table 9 – DeviceIdentityTicketType Structure	24
106	Table 10 – DeviceIdentityTicketType Definition	25
107	Table 11 – CompositIdentityTicketType Structure	25
108	Table 12 – CompositIdentityTicketType Definition	25
109	Table 13 – TicketListType Structure	25
110	Table 14 – TicketListType Definition.....	26
111	Table 15 – CertificateAuthorityType Structure	26
112	Table 16 – CertificateAuthorityType Definition	26
113	Table 17 – DeviceRegistrarType Definition	27
114	Table 18 – Providelidentities Method AddressSpace Definition	29
115	Table 19 – UpdateSoftwareStatus Method AddressSpace Definition	29
116	Table 20 – RegisterDeviceEndpoint Method AddressSpace Definition	30
117	Table 21 – GetManagers Method AddressSpace Definition.....	30
118	Table 22 – ManagerDescription Structure	31
119	Table 23 – ManagerDescription Definition	31
120	Table 24 – RegisterManagedApplication Method AddressSpace Definition	32
121	Table 25 – DeviceRegistrar Definition.....	32
122	Table 26 – DeviceRegistrarAdminType Definition	32
123	Table 27 – RegisterTickets Method AddressSpace Definition	33
124	Table 28 – UnregisterTickets Method AddressSpace Definition	34
125	Table 29 – DeviceRegistrationAuditEventType Definition.....	34
126	Table 30 – DeviceIdentityAcceptedAuditEventType Definition.....	35
127	Table 31 – DeviceSoftwareUpdatedAuditEventType Definition.....	35
128	Table 32 – ProvisionableDevice Object Definition.....	37
129	Table 33 – ProvisionableDeviceType Definition	37
130	Table 34 – RequestTickets Method AddressSpace Definition.....	38
131	Table 35 – SetRegistrarEndpoints Method AddressSpace Definition.....	38
132	Table 36 – ApplicationConfigurationType Definition.....	38
133	Table 37 – NamespaceMetadata Object for this Document.....	39
134	Table 38 – Namespaces used in this document.....	40

135

136

INTERNATIONAL ELECTROTECHNICAL COMMISSION

OPC UNIFIED ARCHITECTURE –

Part 21: Device Onboarding

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

International Standard IEC 62541-21 has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this international standard is based on the following documents:

CDV	Report on voting
65E/XX/CDV	65E/XX/RVC

Full information on the voting for the approval of this international standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Throughout this document and the other Parts of the series, certain document conventions are used:

187 *Italics* are used to denote a defined term or definition that appears in the “Terms and definition” clause
188 in one of the parts of the series.

189 *Italics* are also used to denote the name of a service input or output parameter or the name of a structure
190 or element of a structure that are usually defined in tables.

191 The *italicized terms* and *names* are also often written in camel-case (the practice of writing compound
192 words or phrases in which the elements are joined without spaces, with each element's initial letter
193 capitalized within the compound). For example, the defined term is *AddressSpace* instead of Address
194 Space. This makes it easier to understand that there is a single definition for *AddressSpace*, not
195 separate definitions for Address and Space.

196 A list of all parts of the IEC 62541 series is included in IEC 62541-1 clause 4 Structure of the OPC UA
197 series and published under the general title OPC Unified Architecture, can be found on the IEC website.

198 The committee has decided that the contents of this publication will remain unchanged until the stability
199 date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific
200 publication. At this date, the publication will be

- 201 • reconfirmed,
- 202 • withdrawn,
- 203 • replaced by a revised edition, or
- 204 • amended.

205

206 A bilingual version of this publication may be issued at a later date.

207

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

208

209

210

211

OPC UNIFIED ARCHITECTURE

Part 21: Device Onboarding

1 Scope

This part defines the life cycle of *Devices* and *Composites* and mechanisms to verify their authenticity, set up their security and maintain their configuration.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments and errata) applies.

IEC 62541-1, *OPC Unified Architecture – Part 1: Overview and Concepts*

IEC 62541-2, *OPC Unified Architecture – Part 2: Security*

IEC 62541-3, *OPC Unified Architecture – Part 3: Address Space Model*

IEC 62541-4, *OPC Unified Architecture – Part 4: Services*

IEC 62541-5, *OPC Unified Architecture – Part 5: Information Model*

IEC 62541-6, *OPC Unified Architecture – Part 6: Mappings*

IEC 62541-7, *OPC Unified Architecture – Part 7: Profiles*

IEC 62541-9, *OPC Unified Architecture – Part 9: Alarms and Conditions*

IEC 62541-12, *OPC Unified Architecture – Part 12: Discovery and Global Services*

IEC 62541-14, *OPC Unified Architecture – Part 14: PubSub*

IEC 62541-22, *OPC Unified Architecture – Part 22: Base Network Model*

IEC 62541-100, *OPC Unified Architecture – Part 100: Device Model*

ISO/IEC 11889, Information technology — Trusted platform module library

<https://www.iso.org/standard/66510.html>

802.1AR, Secure Device Identity

<https://1.ieee802.org/security/802-1ar/>

RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

<https://tools.ietf.org/html/rfc3161>

RFC 5280, Internet X.509 Public Key Infrastructure Certificate

<https://tools.ietf.org/html/rfc5280>

RFC 7515, JSON Web Signature (JWS)

<https://tools.ietf.org/html/rfc7515>

RFC 7518, JSON Web Algorithms (JWA)

<https://tools.ietf.org/html/rfc7518>

RFC 2045, Multipurpose Internet Mail Extensions (MIME) Part One

<https://tools.ietf.org/html/rfc2045>

RFC 4648, The Base16, Base32, and Base64 Data Encodings

<https://tools.ietf.org/html/rfc4648>

DIN 91406, Automatic identification of physical objects and information on physical objects in IT systems

<https://www.en-standard.eu/din-spec-91406-automatische-identifikation-von-physischen-objekten-und-informationen-zum-physischen-objekt-in-it-systemen-insbesondere-iiot-systemen-text-deutsch-und-englisch/>

3 Terms, definitions, and conventions

3.1 Terms and definitions

For the purposes of this document the following terms and definitions as well as the terms and definitions given in IEC 62541-1, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-6, IEC 62541-9 and IEC 62541-100 apply.

3.1.1

Application

a program that runs on a *Device* and communicates with other *Applications* on the network.

Note 1 to entry: Each *Application* has an identifier that is unique within the network.

Note 2 to entry: An *OPC UA Application* is an *Application* that supports OPC UA.

3.1.2

ApplicationUri

a globally unique identifier for an *OPC UA Application* running on a particular *Device*.

Note 3 to entry: The *Application Instance Certificate* has the *ApplicationUri* in the *subjectAltName* field.

3.1.3

Composite

a collection of *Devices* or *Composites* assembled into a single unit.

Note 1 to entry: Each *Composite* has a globally unique identifier.

Note 2 to entry: A *Composite* may act as a single *Device* when connected to a network.

Note 3 to entry: A *Composite* may appear as multiple *Devices* when connected to a network.

3.1.4

CompositeBuilder

an organization that creates *Composites*.

3.1.5

CompositeInstanceUri

a globally unique resource identifier assigned by a builder to a *Composite*.

3.1.6

DCA Client

a DCA which is a *Client* and supports *PullManagement*.

3.1.7

DCA Server

a DCA which is a *Server* and supports *PushManagement*.

3.1.8**Device**

As defined in IEC 62541-100.

Note 1 to entry: For this document a *Device* also executes one or more *OPC UA Applications*.

Note 2 to entry: a generic computer or mobile device may be a *Device* if it has a *DeviceIdentity Certificate*

3.1.9**Device Configuration Application (DCA)**

a *Client* or *Server* installed on a *Device* used to configure other applications installed on the same *Device*.

Note 1 to entry: a DCA which is a *Client* uses *PullManagement* (see 7.2) to interact with the *Registrar*.

Note 2 to entry: the *Registrar* uses *PushManagement* (see 7.3) to interact with a DCA which is a *Server*.

3.1.10**DeviceIdentity Certificate**

a *Certificate* issued to a *Device* that identifies the *Device*.

Note 1 to entry: All *DeviceIdentity Certificates* have the *ProductInstanceUri* as a *subjectAltName*.

Note 2 to entry: All *DeviceIdentity Certificates* are IDevID or LDevID Certificates as defined by 802.1AR.

Note 3 to entry: The *ProductInstanceUri* is the *ApplicationUri* when the *DeviceIdentity Certificate* is used to create a *SecureChannel*.

3.1.11**Distributor**

an organization that re-sells *Devices* and/or *Composites*.

Note 1 to entry: A *Distributor* may enhance *Devices* and *Composites* by adding customized products or services.

3.1.12**Manufacturer**

an organization that creates *Devices*.

3.1.13**OwnerOperator**

an organization deploying and operating a system that comprises of *Devices*, *Composites* or other computers connected via a network.

3.1.14**Privilege**

a named set of permissions or access rights which are needed to perform a task.

3.1.15**ProductInstanceUri**

a globally unique resource identifier assigned by the manufacturer to a *Device*.

3.1.16**Registrar**

an *OPC UA Application* that registers and authenticates *Devices* added to the network.

3.1.17**SystemIntegrator**

an organization that installs and configures a system for an *OwnerOperator* that comprises of *Devices*, *Composites* or other computers connected via a network.

3.1.18**SecureElement**

a hardware component that protects *Private Keys* from unauthorized access and disclosure.

3.1.19**Ticket**

a document that identifies a *Device* or *Composite* and has a *DigitalSignature*.

3.2 Abbreviations and symbols

API	Application Programming Interface
ASN.1	Abstract Syntax Notation #1
CA	Certificate Authority
CRL	Certificate Revocation List
DCA	Device Configuration Application
DER	ASN.1 Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ERP	Enterprise Resource Planning
GDS	Global Discovery Server
IDeVID	Initial Device Identifier
LDeVID	Locally Significant Device Identifier
LDS	Local Discovery Server
mDNS	Multicast Domain Name System
NAT	Network Address Translation
PKCS	Public Key Cryptography Standards
TLS	Transport Layer Security
TPM	Trusted Platform Module
UA	Unified Architecture
URI	Uniform Resource Identifier
URN	Uniform Resource Name

4 Onboarding Model

4.1 Device Lifecycle

The Onboarding model is designed to allow the configuration of a *Device* to be managed over the complete lifecycle of the *Device* from manufacture to decommissioning. The entire lifecycle approach is needed because *Devices*, unlike PC-class computers, are often shipped with automation software pre-installed and are connected directly to sensitive networks. This requires a process to authenticate *Devices* before they are given access to a sensitive network.

The complete life cycle of a *Device* is shown in Figure 1.

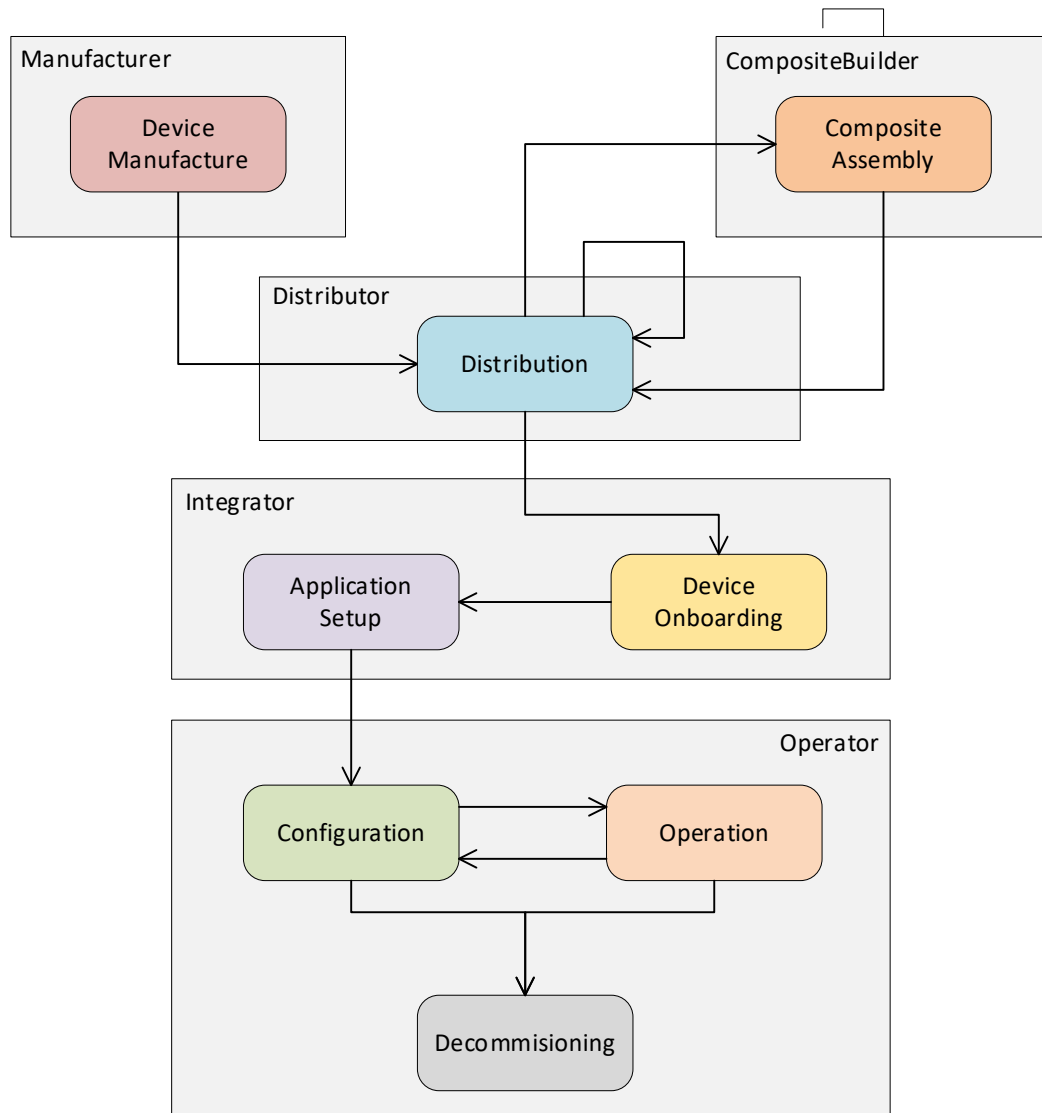


Figure 1 – The Lifecycle of a Device

The actors in the *Device* lifecycle are described in Table 1.

Table 1 – The Actors in the Device Lifecycle

Actor	Description
Device	A computer that is able to communicate via a network. A <i>Device</i> has a unique identifier and may have one or more <i>Applications</i> (see 3.1.4)

Actor	Description
Composite	A collection of <i>Devices</i> or <i>Composites</i> assembled into a single unit. Each <i>Composite</i> has a unique identifier and may appear as a single <i>Device</i> on a network or it may appear as multiple <i>Devices</i> (see 3.1.3).
Application	A program that runs on a <i>Device</i> . Each <i>Application</i> has a unique identifier and communicates with other <i>Applications</i> on the network (see 3.1.1).
OwnerOperator	An organization deploying and operating a system that comprises of <i>Devices</i> , <i>Composites</i> or other computers connected via a network (see 3.1.13).
Manufacturer	An organization that creates <i>Devices</i> (see 3.1.12).
CompositeBuilder	An organization that creates <i>Composites</i> (see 3.1.4).
Distributor	An organization that re-sells <i>Devices</i> and/or <i>Composites</i> . A <i>Distributor</i> enhances <i>Devices</i> and <i>Composites</i> by adding customized products or services before resale (see 3.1.11).
SystemIntegrator	An organization that installs and configures a system for an <i>OwnerOperator</i> that comprises of <i>Devices</i> , <i>Composites</i> or other computers connected via a network (see 3.1.17).
RegistrarAdmin	A user authorized to change the configuration of the <i>Registrar</i> .
SoftwareUpdateAdmin	A user authorized to update the firmware running on a <i>Device</i> .
SecurityAdmin	A user authorized to make changes to security configuration for <i>Clients</i> and <i>Servers</i> running on the network.

The stages in the lifecycle for a single *Device* are described in Table 2. This information model defines mechanisms to automate some of the tasks necessary for each stage.

Table 2 – The Stages in the Device Lifecycle

Stage	Description
Device Manufacture	A <i>Device</i> is created and a <i>DeviceIdentity Certificate</i> is assigned. This <i>Certificate</i> is provided when the <i>Device</i> is transferred to other actors. During <i>Device Manufacture</i> , <i>Applications</i> may be installed on the <i>Device</i> . A <i>Ticket</i> describing the <i>Device</i> is created and signed by the <i>Manufacturer</i> .
Composite Assembly	A <i>Composite</i> is created from <i>Devices</i> and a unique identity is assigned to the <i>Composite</i> . This identity is provided when the <i>Composite</i> is transferred to other actors. During <i>Composite Assembly</i> , <i>Applications</i> may be installed on the <i>Devices</i> contained in the <i>Composite</i> . A <i>Ticket</i> describing the <i>Composite</i> is created and signed by the <i>CompositeBuilder</i> .
Distribution	The <i>Device</i> or <i>Composite</i> is stored until it is delivered to a <i>CompositeBuilder</i> , <i>SystemIntegrator</i> , <i>OwnerOperator</i> or another <i>Distributor</i> .
Onboarding	The <i>SystemIntegrator</i> connects a <i>Device</i> to the network and verifies that the identity reported by the <i>Device</i> matches the identity in a <i>Ticket</i> provided by the <i>Manufacturer</i> or <i>CompositeBuilder</i> .
Application Setup	The <i>SystemIntegrator</i> configures the <i>Applications</i> running on the <i>Device</i> or <i>Composite</i> so they can communicate with other <i>Applications</i> running in the system. This process includes distributing <i>TrustLists</i> and issuing <i>Certificates</i> .
Configuration	The <i>OwnerOperator</i> performs tasks that are not done while the <i>Device</i> is in full operation, such as updating firmware, installing new <i>Applications</i> , or changing <i>Application</i> configuration.
Operation	The <i>Device</i> does the tasks it was deployed to do.
Decommissioning	The <i>Device</i> has all access revoked and, if the <i>Device</i> is still functional, then it is reset to the default factory settings.

The commonly understood concept of “Commissioning” is represented by the *Onboarding*, *Application Setup* and *Configuration* stages.

The stages in the *Device* lifecycle map onto workflows that are defined in this specification. The workflows are described in 4.2.