

SS 695:2023
(ICS 35.020; 35.110; 35.240.01)

SINGAPORE STANDARD

IoT interoperability for Smart Nation



SS 695:2023

(ICS 35.020; 35.110; 35.240.01)

SINGAPORE STANDARD

IoT interoperability for Smart Nation

Published by Enterprise Singapore

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilming, without permission in writing from Enterprise Singapore. Request for permission can be sent to: standards@enterprisesg.gov.sg.

© Enterprise Singapore 2023

ISBN 978-981-5118-67-4

Contents

	Page
Foreword _____	6
0 Introduction _____	7
1 Scope _____	7
2 Normative references _____	7
3 Terms, definitions and abbreviated terms _____	7
4 General _____	10
4.1 IoT in context _____	10
4.2 Guiding principles _____	12
4.3 High-level concerns _____	12
4.4 Architectural concepts _____	13
4.5 IoT interoperability concepts _____	16
4.6 IoT characteristics for interoperability _____	17
4.7 Interworking with other technologies _____	19
4.8 IoT trustworthiness _____	20
5 Requirements for IoT interoperability _____	21
5.1 Unique identification (UID) _____	21
5.2 Modularity (MOD) _____	23
5.3 Network connectivity (NCN) _____	24
5.4 Functional and management capability separation (FMS) _____	27
5.5 Well-defined components (WDC) _____	28
5.6 Composability (CPO) _____	31
5.7 Scalability (SCA) _____	32
5.8 Highly distributed systems (HDS) _____	34
5.9 Shareability (SHA) _____	36
5.10 Heterogeneity (HET) _____	38
5.11 Legacy support (LEG) _____	40
5.12 Data characteristics (DAT) _____	41
5.13 Accuracy (ACC) _____	43
5.14 Network communication (NCM) _____	44
5.15 Real-time capability (RTC) _____	47
5.16 Context-awareness (CTX) _____	48
5.17 Content-awareness (CTN) _____	50
5.18 Self-description (SFD) _____	52
5.19 Discoverability (DSC) _____	54
5.20 Network management and operation (NMO) _____	55
5.21 Manageability (MAN) _____	57

5.22	Auto-configuration (AUT) _____	58
5.23	Service subscription (SSU) _____	60
5.24	Flexibility (FLX) _____	61
5.25	Compliance (CPL) _____	63

Annexes

A	Recommended standards for IoT interoperability _____	65
B	Analysis of recommended standards _____	69
C	Case studies _____	76

Tables

1	IoT characteristics for interoperability _____	17
2	Examples of unique identification _____	21
3	Examples of modularity _____	23
4	Examples of network connectivity _____	25
5	Examples of functional and management capability separation _____	27
6	Examples of well-defined components _____	29
7	Examples of composability _____	31
8	Examples of scalability _____	33
9	Examples of highly distributed systems _____	35
10	Examples of shareability _____	36
11	Examples of heterogeneity _____	38
12	Examples of legacy support” _____	40
13	Examples of data characteristics _____	42
14	Examples of accuracy _____	43
15	Examples of network communication _____	45
16	Examples of real-time capability _____	47
17	Examples of context-awareness _____	49
18	Examples of content-awareness _____	50
19	Examples of self-description _____	52
20	Examples of discoverability _____	54
21	Examples of network management and operation _____	56
22	Examples of manageability _____	57
23	Examples of auto-configuration _____	59
24	Examples of service subscription _____	60
25	Examples of flexibility _____	62
26	Examples of compliance _____	63
A.1	Recommended standards _____	66
B.1	Overview of common standard interfaces _____	69

B.2	Mapping common standard interfaces to 6 aspects _____	69
B.3	Mapping common standard interfaces to IoT architectural characteristics _____	70
B.4	Mapping common standard interfaces to IoT functional characteristics _____	71
B.5	Overview of industry-specific standard interfaces _____	72
B.6	Mapping industry-specific standard interfaces to 6 aspects _____	72
B.7	Mapping industry-specific standard interfaces to IoT architectural characteristics _____	73
B.8	Mapping industry-specific standard interfaces to IoT functional characteristics _____	74
C.1	Architectural characteristics and requirements for passenger hub _____	76
C.2	Functional characteristics and requirements for passenger hub _____	77
C.3	Specific mappings for passenger hub _____	79
C.4	Architectural characteristics and requirements for public safety _____	82
C.5	Functional characteristics and requirements for public safety _____	83
C.6	Specific mappings for public safety _____	85
C.7	Architectural characteristics and requirements for smart facilities _____	87
C.8	Functional characteristics and requirements for smart facilities _____	88
C.9	Specific mappings for smart facilities _____	90
C.10	Architectural characteristics and requirements for smart residential township _____	92
C.11	Functional characteristics and requirements for smart residential township _____	93
C.12	Specific mappings for smart residential township _____	95
C.13	Architectural characteristics and requirements for contact tracing _____	97
C.14	Functional characteristics and requirements for contact tracing _____	98
C.15	Specific mappings for contact tracing _____	99

Figures

1	Examples of use cases for smart city applications _____	11
2	Typical deployment architecture _____	12
3	High-level concerns _____	13
4	IoT logical architecture _____	13
5	IoT interfaces for standardisation _____	15
6	IoT interoperability facets and aspects _____	16
7	IoT characteristics for interoperability and their relationships _____	18
8	IoT interworking with other technologies _____	19
9	Unique identification relationships _____	22
10	Modularity relationships _____	24
11	Network connectivity relationships _____	26
12	Functional and management capability separation relationships _____	28
13	Well-defined components relationships _____	30
14	Composability relationships _____	32
15	Scalability relationships _____	34

16	Highly distributed systems relationships _____	35
17	Shareability relationships _____	37
18	Heterogeneity relationships _____	39
19	Legacy support relationships _____	41
20	Data characteristics relationships _____	42
21	Accuracy relationships _____	44
22	Network communication relationships _____	46
23	Real-time Capability relationships _____	48
24	Context-awareness relationships _____	49
25	Content-awareness relationships _____	51
26	Self-description relationships _____	53
27	Discoverability relationships _____	55
28	Network management and operation relationships _____	56
29	Manageability relationships _____	58
30	Auto-configuration relationships _____	59
31	Service subscription relationships _____	61
32	Flexibility relationships _____	62
33	Compliance relationships _____	64
A.1	Summary of recommended standards _____	65
C.1	Overview of passenger hub solution _____	79
C.2	Selection of technologies for passenger hub _____	80
C.3	High-level solution overview of passenger hub _____	80
C.4	Sample sensor architecture _____	81
C.5	Data sharing across the enterprise using standards _____	81
C.6	Overview of public safety solution _____	84
C.7	High-level solution overview of public safety _____	85
C.8	Overview of smart facilities solution _____	89
C.9	High-level solution overview of smart facilities _____	91
C.10	Overview of smart residential township solution _____	94
C.11	High-level solution overview of smart residential township _____	95
C.12	Detailed functional architecture of smart residential township solution _____	96
C.13	Overview of contact tracing solution _____	99
C.14	High-level solution overview of contact tracing _____	100
C.15	System architecture of contact tracing _____	100
	Bibliography _____	102

Foreword

This Singapore Standard was prepared by the Working Group on IoT Interoperability set up by the Technical Committee on IoT under the purview of the Information Technology Standards Committee.

This SS was developed to facilitate the sharing of IoT data, information, infrastructure and devices across multiple industry applications to support Singapore's Smart Nation vision, by providing design considerations and recommendations for common interface standards applicable for cross-domain applications and nation-wide deployments.

This SS aims to promote the use of IoT standards to lower the barriers of entry by technopreneurs, to foster the development of innovative solution, and to interwork collaboratively with other systems.

In preparing this standard, reference was made to the following publications:

1. ISO/IEC 20924:2021, Information technology – Internet of Things (IoT) – Vocabulary
2. ISO/IEC 30141:2018, Internet of Things (IoT) – Reference architecture
3. ISO/IEC 21823-1:2019, Internet of Things (IoT) – Interoperability for IoT systems – Part 1: Framework

Permission has also been sought from the International Organization for Standardization for the reproduction and adaptation of materials from the standards cited in Clause 3 and ISO/IEC 30141:2018 (as Figures 4 and 5 of this standard).

Acknowledgement is made for the use of information from the above publications.

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all such patent rights.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as "mature standards". Mature standards will not be subject to further review unless there are requests to review such standards.*
2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*
3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

IoT interoperability for Smart Nation

0 Introduction

Connected devices such as smartphones, fitness trackers and remote health monitoring devices have continued to grow as the Internet of Things (IoT) connects more and more devices. As the number of connected devices increases, it is essential that devices, systems, and services from different organisations have some manner of interoperability between themselves to realise the full benefits of IoT.

A smart city is made up of both legacy systems and new projects from different domains. Standards play a critical role in enabling the interconnectivity of these legacy and green-field systems and the sharing of data and information among them.

1 Scope

This standard identifies common requirements for the interoperability of IoT systems, to support a variety of use cases and their integration. It also provides:

- guidance on a minimum set of coherent international and/or industry standards to achieve interoperability. For interoperability, this SS references the IoT architectural and functional characteristics, identified in ISO/IEC 30141:2018 Clause 7, but it does not cover the IoT characteristics for trustworthiness.
- guidance on how interoperability supports the desired characteristics of IoT.
- common requirements for the interoperability of IoT components and solutions.
- case studies to illustrate the recommendations.

It also recommends a minimal set of applicable IoT standards.

2 Normative references

There are no normative references in this standard.