SS 711:2025
(ICS 35.030)

SINGAPORE STANDARD

IoT security for Smart Nation – Concepts and common requirements

Singapore Standards Council

SS 711:2025
(ICS 35.030)

SINGAPORE STANDARD

IoT security for Smart Nation – Concepts and common requirements

Published by Enterprise Singapore

ISBN 978-981-5338-57-7

Contents

Figures

Foreword

This Singapore Standard (SS) was prepared by the Working Group on IoT Security set up by the Technical Committee on Internet of Things under the purview of the Information Technology Standards Committee.

This SS was developed as a result of the review of TR 64:2018. The key changes are as follows:

- Included additional concepts for IoT;
- Updated the list of standard references;
- Updated the list of common requirements; and
- Updated the IoT common vulnerabilities.

This SS aims to:

- safeguard the confidentiality, integrity and availability of large-scale Internet of Things (IoT) systems, and to promote the development of and facilitate mass adoption of such systems;
- establish the foundational security concepts and terminology for IoT systems;
- define a holistic approach for identifying and mitigating the threats and vulnerabilities of IoT systems; and
- provide recommendations on common security requirements for IoT systems.

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

1. SS 695:2023, IoT interoperability for Smart Nation
2. IMDA IoT Cyber Security Guide
3. IMDA IoT Cyber Security Guide Annex A

Permission has also been sought from the following organisations for the reproduction of materials from their publications into this standard:

1. Infocomm Media Development Authority (IMDA)
    - IMDA IoT Cyber Security Guide
    - IMDA IoT Cyber Security Guide Annex A
2. International Electrotechnical Commission (IEC)
    - ISO/IEC 15459-3:2014 Information technology – Automatic identification and data capture techniques – Unique identification
    - ISO/IEC 20924:2024 Internet of Things (IoT) and digital twin – Vocabulary
    - ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary

- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls

- ISO/IEC 27033-1:2015 Information technology – Security techniques – Network security

- ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence

- ISO/IEC 27400:2022 Cybersecurity – IoT security and privacy – Guidelines

- ISO/IEC 27402:2023 Cybersecurity – IoT security and privacy – Device baseline requirements

- ISO/IEC TR 19791:2010 Information technology – Security techniques – Security assessment of operational systems

3. International Organization for Standardization (ISO)

- ISO 21101:2014 Adventure tourism – Safety management systems – Requirements

- ISO/TS 12812-2:2017 Core banking – Mobile financial services – Part 2: Security and data protection for mobile financial services

IEC and ISO standards are available for purchase from Enterprise Singapore.

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 security for Smart Nation – Concepts and common requirements

0 Introduction

The Internet of Things (IoT) seamlessly integrates physical environments with digital objects, facilitating interaction through information and communication (ICT) systems. IoT serves as the foundation for numerous domains utilising sensing and actuation technologies, such as industrial IoT, operational technology (OT), Internet of Medical Things (IoMT), and more. It encompasses a wide array of technologies, including sensing and control, networking, information technology, and software, enabling the interconnection of sensors, actuators, middleware, data, communication networks and applications.

The economic impact of IoT is increasingly evident, with growing adoption in consumer, enterprise, industrial and government sectors, seen in wearables, smart homes, buildings, connected vehicles, and surveillance. As connectivity grows, safeguarding data and managing cybersecurity threats becomes crucial. IoT devices collect significant user and environmental data, requiring protection from vulnerabilities and cyberattacks. Early IoT devices are susceptible to exploitation, posing security concerns and inhibiting user adoption.

Adhering to existing security standards and addressing the scarcity of security expertise within each domain present challenges, underscoring the necessity for practical requirements and guidelines customised to accommodate the dynamic nature of IoT. Safeguarding against cyber threats is crucial for a country's digital economy and the success of its Smart Nation initiatives.

1 Scope

This standard introduces the foundational security concepts and terminology for IoT systems and demonstrates their applications. A holistic approach for identifying and mitigating the threats and vulnerabilities of IoT systems is also outlined. Guidance is provided on how to conduct threat modelling for IoT.

This standard also identifies four basic IoT security design principles (refer to 6.2) and demonstrates their applications. Guidance is also provided on how to classify IoT security requirements and their uses in supporting the identification of security requirements. For each category, security requirements are provided along with examples of how to mitigate common IoT vulnerabilities.

Annex A provides additional information on threat modelling concepts and guidance for IoT, along with an overview of how to apply this standard effectively. Annex B shows how this standard relates to other relevant standards, and Annex C outlines the common vulnerabilities and possible mitigations to these vulnerabilities.

2 Normative references

There are no normative references in this standard.