This is a preview - click here to buy the full publication

TECHNICAL SPECIFICATION

ISO/IEC TS 27570

First edition
2021-01

Privacy protection — Privacy guidelines for smart cities

Reference number
ISO/IEC TS 27570:2021(E)

© ISO/IEC 2021

This is a preview - click here to buy the full publication

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

 © ISO/IEC 2021 – All rights reserved

This is a preview - click here to buy the full publication

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Abbreviated terms **6**

5 Privacy in smart cities **6**
5.1 General 6
5.2 Integration of privacy in the smart city reference framework 6
5.2.1 Smart city ICT reference framework in the ISO/IEC 30145 series 6
5.2.2 Privacy management activities in the ISO/IEC 30145 series 8
5.3 Actors 9
5.4 Challenges 11

6 Guidance on smart city ecosystems privacy protection **13**
6.1 Ecosystem privacy plan 13
6.1.1 Recommendation R6.1 13
6.1.2 Explanations 13
6.1.3 Work product 14
6.2 Governance 14
6.2.1 Recommendation R6.2 14
6.2.2 Explanations 14
6.2.3 Work product 15
6.3 Supply chain 15
6.3.1 Recommendation R6.3 15
6.3.2 Explanations 15
6.3.3 Work product 17
6.4 Data management 17
6.4.1 Recommendation R6.4 17
6.4.2 Explanations 17
6.4.3 Work product 18

7 Guidance on standards for smart city ecosystems privacy protection **18**
7.1 General 18
7.2 Privacy governance 19
7.3 Privacy risk management 20
7.4 Privacy engineering 20

8 Guidance on processes for smart city ecosystem privacy protection **20**
8.1 General 20
8.2 Governance process 21
8.2.1 Recommendation R8.2 21
8.2.2 Explanations 21
8.2.3 Guidance on ecosystem coordination 21
8.2.4 Guidance for organizations 22
8.2.5 Standards and methods 22
8.2.6 Work product 22
8.3 Data management process 23
8.3.1 Recommendation R8.3 23
8.3.2 Explanations 23
8.3.3 Guidance on ecosystem coordination 23
8.3.4 Guidance for organizations 23
8.3.5 Standards and methods 24
8.3.6 Work product 24

© ISO/IEC 2021 – All rights reserved

This is a preview - click here to buy the full publication

8.4 Risk management process ... 24
8.4.1 Recommendation R8.4 ... 24
8.4.2 Explanations ... 24
8.4.3 Guidance for ecosystem coordination ... 25
8.4.4 Guidance for organizations ... 25
8.4.5 Standards and methods ... 26
8.4.6 Work product ... 26
8.5 Engineering process ... 26
8.5.1 Recommendation R8.5 ... 26
8.5.2 Explanations ... 27
8.5.3 Guidance for ecosystem coordination ... 27
8.5.4 Guidance for organizations ... 28
8.5.5 Standards and methods ... 28
8.5.6 Work product ... 29
8.6 Citizen engagement process ... 29
8.6.1 Recommendation R8.6 ... 29
8.6.2 Explanations ... 29
8.6.3 Guidance for ecosystem coordination ... 29
8.6.4 Guidance for organizations ... 30
8.6.5 Work product ... 31

Annex A (informative) **Example of ecosystem privacy plan structure** ... **32**

Annex B (informative) **Using video cameras in smart cities** ... **34**

Bibliography ... **36**

© ISO/IEC 2021 – All rights reserved

This is a preview - click here to buy the full publication

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2021 – All rights reserved

This is a preview - click here to buy the full publication

Introduction

The growing integration of ICT technologies (e.g. cloud computing, IoT, big data, mobile networks, artificial intelligence and machine learning) in smart cities will allow for improved data sharing capabilities to achieve better services. But the growing complexity of the ICT infrastructure will also create vulnerabilities at security and privacy level. Security incidents can lead to essential services not operating properly, for instance a massive electricity supply shortage. Likewise, unauthorized access to personal data can lead to major privacy breaches, for instance access to personal health data records.

Ensuring that privacy is properly dealt within smart cities is a challenge. First, a wide variety of public and private stakeholders can be involved such as:

— agencies in charge of managing essential city services for instance administration services;

— business organizations in charge of operating services for instance electricity distribution:

— organizations in supply chains associated with the deployment of related infrastructure for instance transport systems; and

— associations representing the viewpoints of citizens.

Secondly, a wide variety of standards can be used such as:

— privacy standards;

— smart city standards;

— cloud computing standards;

— IoT standards;

— big data standards; and

— IT governance standards.

Figure 1 shows examples of such standards. This document thus focuses on providing guidance on the use of standards, while taking into account the variety of stakeholders in a smart city ecosystem.

© ISO/IEC 2021 – All rights reserved

This is a preview - click here to buy the full publication

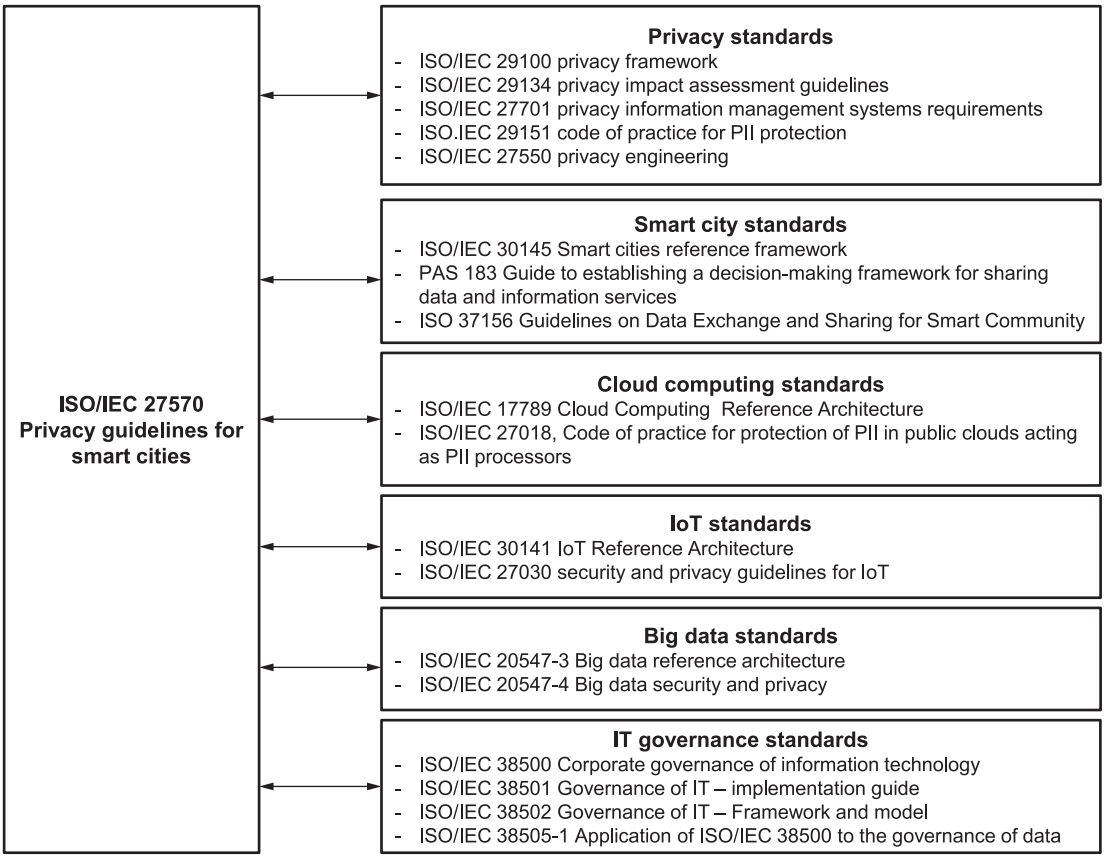

Figure 1 — Examples of standards to reference

Figure 2 summarizes privacy recommendations to smart cities ecosystems in this document, further numbered R6.1, R6.2, R6.3, and R6.4.

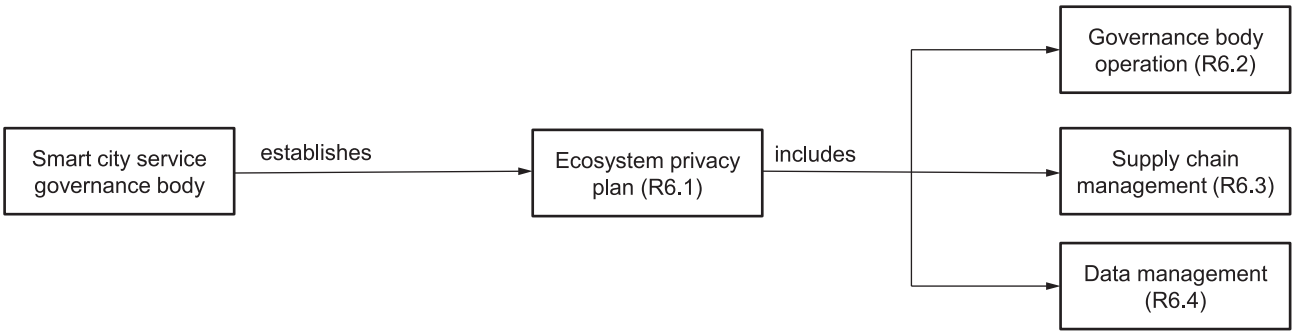

Figure 2 — Ecosystem guidance for privacy

Figure 3 summarizes privacy recommendations to smart cities processes in this document, further numbered R8.2, R8.3, R8.3, R8.4, and R8.5.

© ISO/IEC 2021 – All rights reserved

This is a preview - click here to buy the full publication

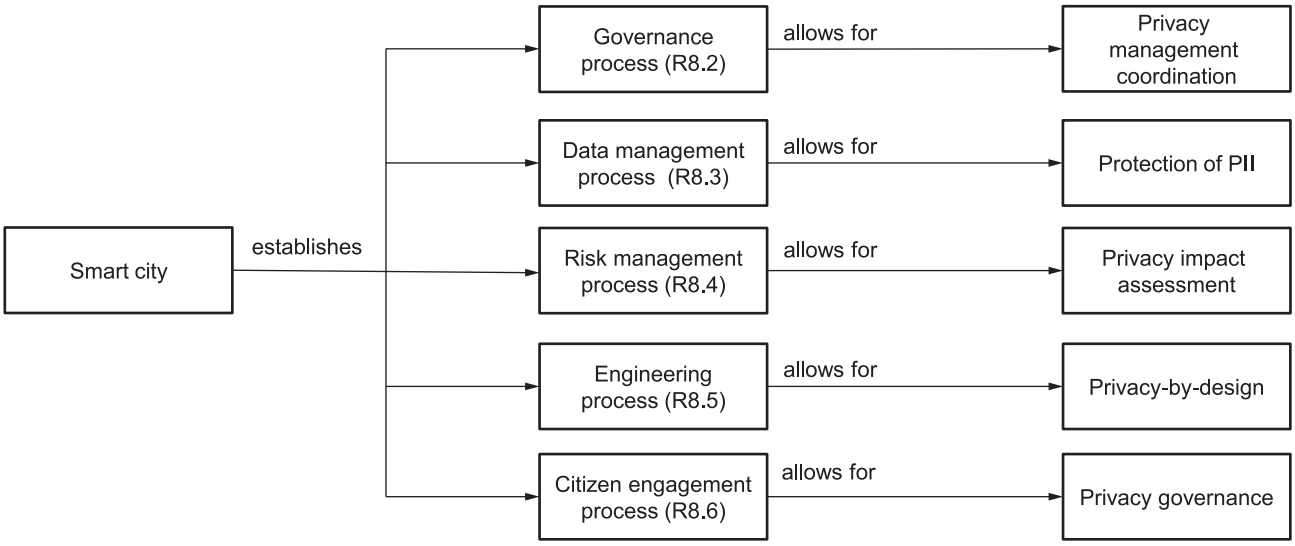

Figure 3 — Process guidance for privacy

It is foreseen that this document will pave the way to future privacy standards for smart cities. Table 1 provides a list of possible future standards.

Table 1 — Examples of possible future standards

Category	Standards
Privacy management to keep track and monitor PII assets that are exploited in smart cities.	Framework for privacy management in smart cities Guidelines for communication between organizations Guidelines for privacy management plans in smart cities Guidelines for privacy policy making in smart cities including data retention Guidelines for privacy impact assessment reports in smart cities Guidelines for consent management in smart cities Guidelines for privacy accountability and transparency management in smart cities Guidelines for privacy breach management in smart cities Guidelines for privacy-by-design of smart city services Guidelines for the integration of privacy concerns in data exchange agreements Smart city services security and privacy assurance
Privacy engineering in smart city ecosystems	Guidelines for privacy engineering[a] in smart cities
Collaboration in smart city ecosystems	Guidelines for citizen engagement Guidelines for communication between organizations (for each type of organization, e.g. administration)
Interoperability to avoid vendor lock-in	Common privacy management information model in smart cities Common privacy impact assessment information in smart cities Common description of privacy capabilities in smart cities Common description of privacy incidents in smart cities

[a] Privacy engineering focuses on the integration of privacy concerns in the engineering of a system.

© ISO/IEC 2021 – All rights reserved

This is a preview - click here to buy the full publication

Privacy protection — Privacy guidelines for smart cities

1 Scope

The document takes a multiple agency as well as a citizen-centric viewpoint.

It provides guidance on:

— smart city ecosystem privacy protection;

— how standards can be used at a global level and at an organizational level for the benefit of citizens; and

— processes for smart city ecosystem privacy protection.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations that provide services in smart city environments.

2 Normative references

There are no normative references in this document.

© ISO/IEC 2021 – All rights reserved