Technical Specification

ISO/IEC TS 27564

Privacy protection — Guidance on the use of models for privacy engineering

Protection de la vie privée — Recommandations relatives à l'utilisation de modèles pour l'ingénierie de la vie privée

First edition
2025-09

Reference number
ISO/IEC TS 27564:2025(en)

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **2**
5 Engineering with models ... **3**
5.1 Models ... 3
5.2 MBSSE (model-based systems and software engineering) ... 5
6 Privacy engineering with models ... **7**
6.1 Privacy models ... 7
6.1.1 Guidance on models ... 7
6.1.2 Model intellectual property rights ... 8
6.1.3 Models representation, storage and reuse ... 8
6.1.4 Models for behavioural and policy interoperability ... 8
6.2 Privacy engineering models of interest ... 8
6.3 Privacy engineering supported by MBSSE ... 9
6.4 Initiatives and standards of interest ... 12
7 Guidance on the use of privacy models ... **13**
7.1 Engineering privacy capabilities ... 13
7.2 Integrating the context of a system of interest ... 14
7.3 Supporting systems of systems emerging risks ... 14
7.4 Integration of horizontal standards ... 16
Annex A (informative) **Using models for privacy engineering — Examples** ... **19**
Bibliography ... **31**

© ISO/IEC 2025 – All rights reserved

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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 and www.iec.ch/national-committees.

© ISO/IEC 2025 – All rights reserved

Introduction

Systems that process personal information are and continue to become more complex. This is due to an increasing ability to analyse, use, and store growing volumes of data. This complexity introduces greater privacy risks for the individuals to whom this data pertains. Embedding privacy into these complex systems is ever more important and provides an approach that mitigates these risks through system design. Model-based systems and software-based engineering (MBSSE) provides such an approach to the discipline of privacy engineering. Adding privacy modelling to the roster of tools to identify and assess privacy risks and support potential risk mitigation strategies will help connect a concept to reality, i.e. the value of making privacy and data protection a priority. Incorporating MBSSE into privacy engineering enables a complex system to achieve both privacy and functionality in an easy-to-understand manner.

This document introduces the concept of MBSSE in the context of privacy engineering and provides technical guidance on the use of engineering models for privacy engineering. The technical guidance is illustrated by sample use cases taken from ISO/IEC TR 31700-2[1] and a use case on privacy threat modelling.

Clause 5 explains the model-based system and software engineering (MBSSE) and the benefits of using models as a single source of truth (SSOT), including:

— consistency, ensured throughout the system lifecycle, as models can be transmitted from one lifecycle stage to another, and used by engineering tools;

— interoperability, as models can be dynamically exchanged between systems in operation.

Clause 6 explains how MBSSE can be applied to privacy engineering by:

— explaining the benefit of privacy models and their management;

— identifying privacy models of interest, taking a system, ecosystem and an engineering perspective;

— showing how ISO/IEC/IEEE 24641[2] can be customized for privacy engineering;

— listing initiatives and standards of interest for privacy engineering with models.

Clause 7 elaborates on models by:

— explaining privacy capabilities, considering the relationship between a system of interest (subject to system engineering) and a privacy capability (subject to privacy engineering);

— explaining the intended context of a system of interest;

— describing emerging behaviour at system engineering level in the case of systems of systems, and describing associated privacy capabilities at privacy engineering level;

— explaining how to construct models through a profile approach in order to support the interplay with transversal standards (e.g. technology standards on AI or IoT, or cross-cutting standards on safety or resilience);

— providing guidance through sample use cases taken from ISO/IEC TR 31700-2, focusing on privacy threat models.

© ISO/IEC 2025 – All rights reserved

Privacy protection — Guidance on the use of models for privacy engineering

1 Scope

This document provides guidance on how to use modelling in privacy engineering.

It describes categories of models that can be used, the use of modelling to support engineering, and the relationships with other references, including International Standards on privacy engineering and on modelling.

It provides high-level use cases describing how models are used.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
capability
ability to do something useful under a particular set of conditions

Note 1 to entry: Generally, different kinds of capabilities exist: organizational capability, system capability and operational capability.

[SOURCE: ISO/IEC/IEEE 24641:2023, 3.1.3, modified — Note to entry simplified.]

3.2
model
abstract representation of an entity or collection of entities that provides the ability to portray, understand or predict the properties or characteristics of the entity or collection under conditions or situations of interest

Note 1 to entry: A model can use a formalism that could be based on mathematical or scientific principles and concepts. A model can be generated using an established metamodel. Metamodels are often used to facilitate development of accurate, complete, consistent and understandable models.

Note 2 to entry: A model can be used to construct or express architecture views of the entity. Descriptive models and analytic models are two kinds of models. A model should be governed by a model kind in accordance with ISO/IEC/IEEE 42010.

Note 3 to entry: A reference model can be used to capture a general case that is used as the basis for creating special case models for particular conditions or situations. A reference model can be used to encourage and enforce uniformity of architectures and architecture elements.

© ISO/IEC 2025 – All rights reserved

Note 4 to entry: The model can be an architecture model, architecture entity model, concept model or reference model, as the case may be.

Note 5 to entry: A physical model is a concrete representation that is distinguished from the mathematical and logical models, both of which are more abstract representations of the system. The abstract model can be further classified as descriptive (similar to logical) or analytical (similar to mathematical).

Note 6 to entry: Models can have other models as components.

Note 7 to entry: Models can be presented at different levels of abstraction to facilitate understanding and cooperation between stakeholders and practioners at different levels.

[SOURCE: ISO/IEC/IEEE 42020:2019, 3.13, modified — Notes 5, 6 and 7 to entry added.]

3.3
model pattern
general, reusable *model* (3.2) or model part that can be used as a solution to a commonly occurring problem within a given context in system or software design

[SOURCE: ISO/IEC/IEEE 24641:2023, 3.1.21]

3.4
repository
place where, or receptacle in which, things are or can be stored

[SOURCE: ISO/IEC 19763-1:2023, 3.13, modified — Note to entry deleted.]

3.5
model repository
repository (3.4) where *models* (3.2) are stored

[SOURCE: ISO/IEC 19763-1:2023, 3.11]

4 Abbreviated terms

AI	artificial intelligence
CPRA	California Privacy Rights Act
DPIA	data protection impact assessment
DPM	data privacy management
DPMF	data protection modelling framework
DPV	data privacy vocabulary
EMT	epistimis modelling tool
GDPR	general data protection regulation
IPR	intellectual property rights
JSON	JavaScript™ [1] Object Notation

JavaScript™ is the trademark of a product supplied by Oracle® Corporation. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

© ISO/IEC 2025 – All rights reserved