TECHNICAL REPORT

ISO/IEC TR 27550

First edition
2019-09

Information technology — Security techniques — Privacy engineering for system life cycle processes

Technologies de l'information — Techniques de sécurité — Ingénierie de la vie privée pour les processus du cycle de vie des systèmes

Reference number
ISO/IEC TR 27550:2019(E)

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviated terms ... **4**

5 Privacy engineering ... **5**

5.1 General ... 5

5.2 Relationship with system and software engineering ... 5

5.3 Relationship with security engineering ... 6

5.4 Relationship with risk management ... 7

6 Integration of privacy engineering in ISO/IEC/IEEE 15288 ... **9**

6.1 General ... 9

6.2 Acquisition and supply processes ... 10

6.3 Human resources management process ... 11

6.4 Knowledge management process ... 12

6.5 Risk management process ... 14

6.6 Stakeholder needs and requirements definition process ... 16

6.7 System requirements definition process ... 17

6.8 Architecture definition process ... 19

6.9 Design definition process ... 21

Annex A (informative) **Additional guidance for privacy engineering objectives** ... **24**

Annex B (informative) **Additional guidance for privacy engineering practice** ... **28**

Annex C (informative) **Catalogues** ... **35**

Annex D (informative) **Examples of risk models and methodologies** ... **45**

Bibliography ... **50**

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 http://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*.

Introduction

Privacy engineering is often associated with terms such as:

— privacy-by-design and privacy-by-default, coined by Ann Cavoukian[16] in the early nineties; or

— data protection by design and data protection by default, used in the European regulation published in April 2016[17].

In recent years, a number of concepts, principles and approaches have been proposed for privacy engineering. In a paper on privacy engineering[20], Spiekermann and Cranor contrast privacy-by-architecture from privacy-by-policy. The former focuses on data minimization, anonymization and client-side data processing and storage while the latter focuses on enforcing policies in data processing. In a paper on engineering privacy-by-design[21], Gürses, Troncoso, and Diaz state that data minimization should be the foundational principle for engineering privacy-respecting systems. In a paper on privacy-by-design in intelligent transport systems[22], Kung, Freytag and Kargl define three principles, minimization, enforcement and transparency. In a paper on protection goals for privacy engineering[23], Hansen, Jensen, and Rost identify three goals: unlinkability, transparency and intervenability. In two papers on privacy design strategies[29][30], Hoepman identifies four data oriented strategies (minimize, separate, abstract, hide), as well as four process oriented strategies (inform, control, enforce, demonstrate).

A number of global papers have been published. A privacy threat framework was defined by KU Leuven[24] that led to the LINDDUN methodology[25]. Two OASIS technical committees published specifications focusing on the implementation of privacy in systems: the *Privacy Management Reference Model and Methodology* (July 2013, updated in May 2016)[27] and the *Privacy by Design Documentation for Software Engineers* and *Companion committee note* published in June 2014[28]. The December 2014 ENISA report entitled *Privacy and Data Protection by Design — from Policy to Engineering*[26] provides a good overview on privacy policies and their influence on the definition of privacy engineering concepts. The December 2015 privacy and security-by-design methodology handbook from PRIPARE[31] provides a methodology which covers the whole engineering lifecycle integrating existing concepts, principles and methods. Joyee De and Le Métayer published in 2016 a book on privacy risk analysis[32]. The January 2017 NIST internal report[19] introduces a definition of privacy engineering, a privacy risk model and three privacy engineering objectives: predictability, manageability and disassociability.

Privacy engineering practice is supported by a growing body of standards on privacy, on security, and on software and system engineering.

Examples of useful privacy standards are:

— ISO/IEC 29100[10] which provides a high-level framework for the protection of PII within ICT systems. It is general in nature and places organizational, technical, and procedural aspects in an overall privacy framework;

— ISO/IEC 29134[11] which gives guidelines for a process on privacy impact assessments (PIA) and a structure and content of a PIA report;

— ISO/IEC 29151[12] which establishes control objectives, controls and guidelines for implementing controls to meet the requirements identified by a risk and impact assessment related to the protection of PII;

— ISO/IEC 27018[13] which defines a code of practice for the protection of personally identifiable information (PII) in public clouds acting as PII processors;

— ISO/IEC 27552[14] which provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS); and

— OASIS privacy management reference model and methodology (PMRM)[27] which provides a guideline or template for developing operational solutions to privacy issues.

When the security of personally identifiable information (PII) is at stake, privacy engineering can be supported by security standards such as:

— ISO/IEC 27001[6] which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization;

— ISO/IEC 27002[7] which provides guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls;

— ISO/IEC 27005[8] on information security risk management which can be used as a reference for privacy risk management processes; and

— ISO/IEC 27034[9] on application security which can be used to assist organizations in integrating security concerns related to PII throughout the life cycle of their applications.

When the engineering of software products and systems is involved, privacy engineering can be supported by software and system engineering standards such as:

— ISO/IEC/IEEE 15288[1] on system life cycle processes which can be used to describe privacy engineering processes;

— ISO/IEC/IEEE 12207[2] on software life cycle processes; and

— ISO/IEC/IEEE 29148[3] on requirement engineering which can be used for the engineering of privacy requirements for systems and software products and services throughout the life cycle.

This document takes into account principles and concepts for privacy engineering as well as standards and practices related to privacy, security and system and software engineering. It extends ISO/IEC/IEEE 15288 by adding specific guidelines that will help organizations integrate advances in privacy engineering in their engineering practices.

Privacy engineering practice is also influenced by the following factors:

— the need to adapt privacy engineering to different system and software engineering practices such as agile programming;

— the need to have a multidisciplinary approach integrating different viewpoints such as citizen, societal, ethical, legal, technical, or business viewpoints;

— the need to adapt privacy engineering to the different organizational roles in a supply chain such as a system developer, a system integrator, or a system operator;

— the need to take into account the specific system and application needs of a sector such as smart grids, health, or transport; and

— the various interactions that engineers need to have with other stakeholders (e.g., product owner, system product manager, privacy officer) to take into account the multidisciplinary facets of privacy engineering.

This document also contains guidance on how an organization can adapt its privacy engineering practices to take into account these specific factors. Since this document is intended to encourage good privacy practice in the development of a wide range of ICT systems and applications, it does not contain system specific or application specific content.

