SLOVENSKI STANDARD
SIST EN ISO/IEC 29101:2021

01-december-2021

Informacijska tehnologija - Varnostne tehnike - Okvir arhitekture zasebnosti (ISO/IEC 29101:2018)

Information technology - Security techniques - Privacy architecture framework (ISO/IEC 29101:2018)

Informationstechnik - Sicherheitstechniken - Rahmenwerk für Datenschutz (ISO/IEC 29101:2018)

Technologies de l'information - Techniques de sécurité - Architecture de référence de la protection de la vie privée (ISO/IEC 29101:2018)

Ta slovenski standard je istoveten z: **EN ISO/IEC 29101:2021**

ICS:

35.030	Informacijska varnost	IT Security

SIST EN ISO/IEC 29101:2021 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 29101

October 2021

ICS 35.030

English version

Information technology - Security techniques - Privacy architecture framework (ISO/IEC 29101:2018)

Technologies de l'information - Techniques de sécurité - Architecture de référence de la protection de la vie privée (ISO/IEC 29101:2018)

Informationstechnik - Sicherheitstechniken - Rahmenwerk für Datenschutz (ISO/IEC 29101:2018)

This European Standard was approved by CEN on 27 September 2021.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Ref. No. EN ISO/IEC 29101:2021 E

Contents

Page

European foreword

The text of ISO/IEC 29101:2018 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 29101:2021 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2022, and conflicting national standards shall be withdrawn at the latest by April 2022.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 29101:2018 has been approved by CEN-CENELEC as EN ISO/IEC 29101:2021 without any modification.

INTERNATIONAL STANDARD

ISO/IEC 29101

Second edition
2018-11

Information technology — Security techniques — Privacy architecture framework

Technologies de l'information — Techniques de sécurité — Architecture de référence de la protection de la vie privée

Reference number
ISO/IEC 29101:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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 Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 29101:2013) which has been technically revised. The main change compared to the previous edition is that old Annex D has been removed.

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.

Introduction

This document describes a high-level architecture framework and associated controls for the safeguarding of privacy in information and communication technology (ICT) systems that store and process personally identifiable information (PII).

The privacy architecture framework described in this document:

— provides a consistent, high-level approach to the implementation of privacy controls for the processing of PII in ICT systems;

— provides guidance for planning, designing and building ICT system architectures that safeguard the privacy of PII principals by controlling the processing, access and transfer of personally identifiable information; and

— shows how privacy enhancing technologies (PETs) can be used as privacy controls.

This document builds on the privacy framework provided by ISO/IEC 29100 to help an organization define its privacy safeguarding requirements as they relate to PII processed by any ICT system. In some countries, privacy safeguarding requirements are understood to be synonymous with data protection/privacy requirements and are the subject of data protection/privacy legislation.

Information technology — Security techniques — Privacy architecture framework

1 Scope

This document defines a privacy architecture framework that:

— specifies concerns for ICT systems that process PII;

— lists components for the implementation of such systems; and

— provides architectural views contextualizing these components.

This document is applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating ICT systems that process PII.

It focuses primarily on ICT systems that are designed to interact with PII principals.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

ISO/IEC/IEEE 42010, *Systems and software engineering — Architecture description*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100 and ISO/IEC/IEEE 42010 apply.

4 Symbols and abbreviated terms

The following abbreviations apply to this document.

ICT Information and Communication Technology

PET Privacy Enhancing Technology

PII Personally Identifiable Information

5 Overview of the privacy architecture framework

5.1 Elements of the framework

The privacy architecture framework presented in this document is intended as a technical reference for developers of ICT systems that process PII. This document does not set requirements for privacy policies; it assumes that a privacy policy is in place and that privacy safeguarding requirements have been defined and that appropriate safeguards are implemented within the ICT system.

This architecture framework focuses on the protection of PII. Since this is partly a security goal, ICT systems processing PII should also follow information security engineering guidelines. This architecture framework lists some information security components that are critical for safeguarding PII processed within ICT systems. The architecture framework presented is based on the model used in ISO/IEC/IEEE 42010.

The stakeholders related to these concerns are the privacy stakeholders defined in ISO/IEC 29100. They are discussed in more detail in Clause 6.

The concerns for the architecture framework are described in Clause 7 and include the privacy principles of ISO/IEC 29100 and privacy safeguarding requirements specific to an ICT system.

The architecture framework is presented as follows:

a) the layers of the technical architecture framework in 8.2 show the architecture from a component viewpoint. Each layer groups components with a common goal or a similar function;

b) the deployment model in 8.3 shows the architecture framework from a standalone ICT system viewpoint. Each view shows a grouping of the components based on their deployment in the stakeholders' ICT systems; and

c) the views in 8.4 show the architecture framework from an interaction viewpoint. The views illustrate how the components interact between ICT systems of different stakeholders.

The architecture framework also presents correspondence rules between the concerns and viewpoints through the use of mapping tables.

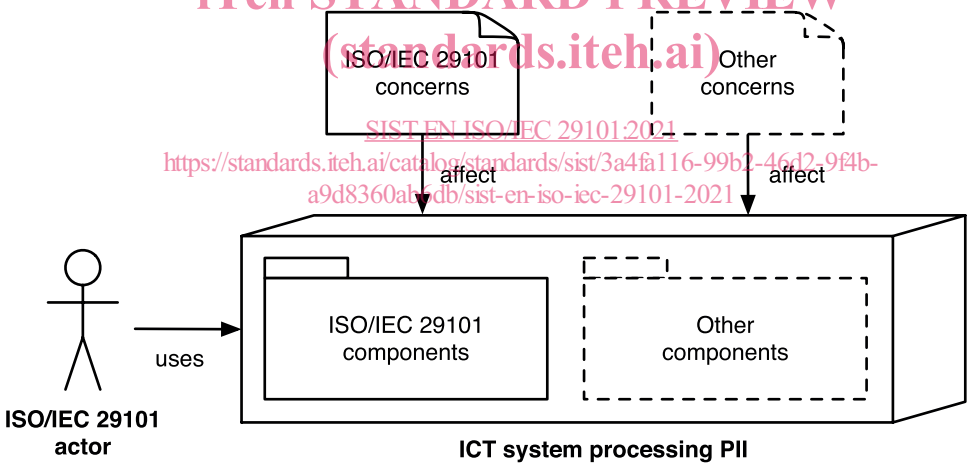

Figure 1 — Elements of the privacy architecture framework in context

Figure 1 illustrates the relationship between the elements of the privacy architecture framework. The central element of the architecture framework is the ICT system being built. An ISO/IEC 29101 actor uses the ICT system. The design of the ICT systems is affected by both concerns addressed in this document and also other concerns. Examples of other concerns include non-functional requirements that affect the performance, accessibility and design of the ICT system and do not affect the functional processing of PII. These other concerns are out of the scope of this document.

The ICT system can contain components from the privacy architecture framework of this document as well as other components. These components do not process PII, but instead handle other functionality in the ICT system like providing accessibility or rendering special user interfaces. Such components are out of the scope of this document.

5.2 Relationship with management systems

The use of a management system enables PII controllers and processors to more effectively meet their privacy safeguarding requirements using a structured approach. This structured approach also provides PII controllers and processors the ability to measure outcomes and continuously improve the management system's effectiveness.

An effective management system is as transparent as possible but still impacts people, processes and technology. It should be part of the internal control program and risk mitigation strategy of an organization and its implementation helps to satisfy compliance with data protection and privacy regulations.

6 Actors and PII

6.1 Overview

The actors of the ISO/IEC architecture framework are the privacy stakeholders involved in PII processing described in ISO/IEC 29100. These actors are:

a) the PII principal;

b) the PII controller; and

c) the PII processor.

NOTE The "third party" defined as one of the four categories of the actors in ISO/IEC 29100 is out of the scope of the architecture framework specified in this document.

From the deployment viewpoint, the architecture framework is divided into three parts. Each part applies to the ICT system deployed from the viewpoint of each of these actors.

Figure 2 shows the ICT systems of the actors and the flows of PII between these ICT systems. It illustrates the logical division of functionality for the architecture framework described in this document. It is not intended as a representation of the physical structure, organisation or ownership of ICT system hardware.

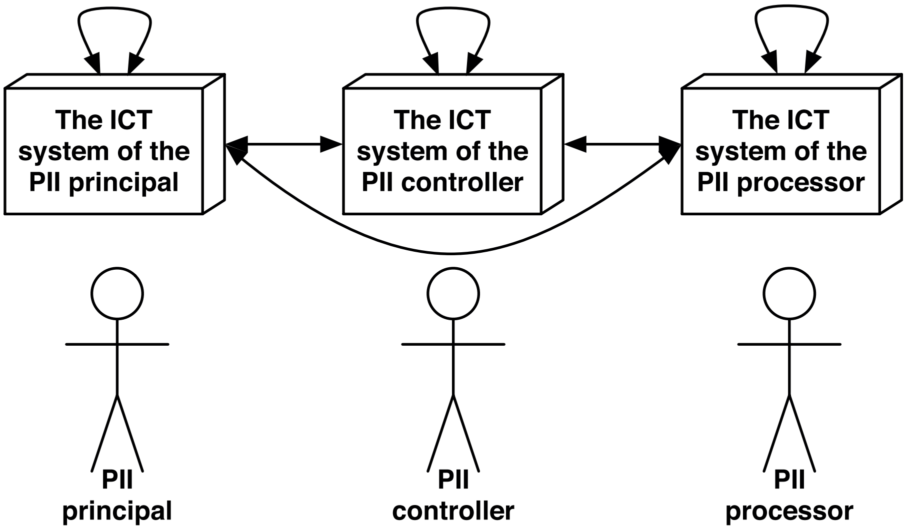

Figure 2 — Actors and their ICT systems according to this document

An actor can be responsible for building the ICT systems that it uses, or not. For example, the PII principal can use a system built by and the responsibility of the PII controller or the ICT system of the PII principal can be a part of the ICT system of the PII controller. Furthermore, the functionality of the ICT system