

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 29101:2021 sisaldab Euroopa standardi EN ISO/IEC 29101:2021 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 29101:2021 consists of the English text of the European standard EN ISO/IEC 29101:2021.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 13.10.2021.	Date of Availability of the European standard is 13.10.2021.
Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis- ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autoriõiguse kaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about standards copyright protection, please contact the Estonian Centre for Standardisation and Accreditation: Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

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

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.

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	1
5 Overview of the privacy architecture framework	1
5.1 Elements of the framework	1
5.2 Relationship with management systems	3
6 Actors and PII	3
6.1 Overview	3
6.2 Phases of the PII processing life cycle	4
6.2.1 Collection	4
6.2.2 Transfer	5
6.2.3 Use	5
6.2.4 Storage	6
6.2.5 Disposal	6
7 Concerns	6
7.1 Overview	6
7.2 The privacy principles of ISO/IEC 29100	6
7.3 Privacy safeguarding requirements	7
8 Architectural views	7
8.1 General	7
8.2 Component view	8
8.2.1 General	8
8.2.2 Privacy settings layer	9
8.2.3 Identity management and access management layer	12
8.2.4 PII layer	14
8.3 Actor view	19
8.3.1 General	19
8.3.2 ICT system of the PII principal	20
8.3.3 ICT system of the PII controller	20
8.3.4 ICT system of the PII processor	21
8.4 Interaction view	22
8.4.1 General	22
8.4.2 Privacy settings layer	22
8.4.3 Identity and access management layer	23
8.4.4 PII layer	23
Annex A (informative) Examples of the PII-related concerns of an ICT system	25
Annex B (informative) A PII aggregation system with secure computation	30
Annex C (informative) A privacy-friendly, pseudonymous system for identity and access control management	37

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.