
**Information technology — Security
techniques — Privacy architecture
framework**

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

This document is a preview generated by PVSS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013

All rights reserved. Unless otherwise specified, 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
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction.....	vi
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	2
5.1 Elements of the framework.....	2
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.....	7
7.3 Privacy safeguarding requirements	7
8 Architectural views.....	8
8.1 Introduction.....	8
8.2 Component view.....	8
8.2.1 Privacy settings layer.....	9
8.2.2 Identity management and access management layer.....	12
8.2.3 PII layer.....	14
8.3 Actor view.....	21
8.3.1 ICT system of the PII principal	21
8.3.2 ICT system of the PII controller	21
8.3.3 ICT system of the PII processor.....	22
8.4 Interaction view	23
8.4.1 Privacy settings layer.....	23
8.4.2 Identity and access management layer.....	24
8.4.3 PII layer.....	24
Annex A (informative) Examples of the PII-related concerns of an ICT system.....	26
Annex B (informative) A PII aggregation system with secure computation	32
Annex C (informative) A privacy-friendly, pseudonymous system for identity and access control management	39
Annex D (informative) Relating privacy principles to information security controls	45

Figures

Figure 1 — Elements of the privacy architecture framework in context	2
Figure 2 — The actors and their ICT systems according to ISO/IEC 29101	4
Figure 3 — The architecture of the ICT system of the PII principal.....	21
Figure 4 — The architecture of the ICT system of the PII controller	22
Figure 5 — The architecture of the ICT system of the PII processor	23
Figure 6 — The deployment of components in the privacy settings layer.....	24
Figure 7 — The deployment of components in the identity and access management layer.....	24
Figure 8 — The deployment of components in the PII layer	25
Figure B.1 — Deployment of the secure computation system	33
Figure B.2 — The architecture for the PII entry ICT system.....	33
Figure B.3 — The architecture for the study coordinator ICT system	35
Figure B.4 — The architecture for the secure data analysis application	36
Figure C.1 — An overview of the architecture – actors and their interactions	40
Figure C.2 — Architecture of the ICT system of the University Credential Issuer.....	41
Figure C.3 — Architecture of the ICT system of the student.....	42
Figure C.4 — Architecture of the Course Evaluation Application.....	43

Tables

Table 1 — Example of the relationship between privacy principles and the components in the privacy settings layer	12
Table 2 — Example of the relationship between privacy principles and the components in the identity and access management layer.....	15
Table 3 — Example of the relationship between privacy principles and the components in the PII layer	20
Table A.1 — Examples of the relationship between concerns and the components in the privacy settings layer	29
Table A.2 — Examples of the relationship between concerns and the components in the identity and access management layer.....	29
Table A.3 — Examples of the relationship between concerns and the components in the PII layer	30
Table A.4 — Examples of the relationship between privacy principles and the high-level concerns.....	31
Table D.1 — Privacy principles and their corresponding information security controls	45

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 29101 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Introduction

This International Standard 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 International Standard

- 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 International Standard 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.

This International Standard focuses on ICT systems that are designed to interact with PII principals.

Information technology — Security techniques — Privacy architecture framework

1 Scope

This International Standard 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 International Standard 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, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

ISO/IEC/IEEE 42010:2011, *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 ISO/IEC 29101:

ICT	Information and Communication Technology
PET	Privacy Enhancing Technology
PII	Personally Identifiable Information