BS ISO/IEC 29101:2013

BSI Standards Publication

Information technology — Security techniques — Privacy architecture framework

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 29101:2013

National foreword

This British Standard is the UK implementation of ISO/IEC 29101:2013.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2013. Published by BSI Standards Limited 2013

ISBN 978 0 580 59542 4

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2013.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 29101:2013

INTERNATIONAL STANDARD

ISO/IEC 29101

First edition
2013-10-15

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 29101:2013(E)

Documents
Document Sharing Hub

© ISO/IEC 2013

Full document details: BS ISO/IEC 29101:2013

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

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 29101:2013

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

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 29101:2013

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

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 29101:2013

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*.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

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.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

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

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

5 Overview of the privacy architecture framework

5.1 Elements of the framework

The privacy architecture framework presented in ISO/IEC 29101 is intended as a technical reference for developers of ICT systems that process PII. This standard 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 will be 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.

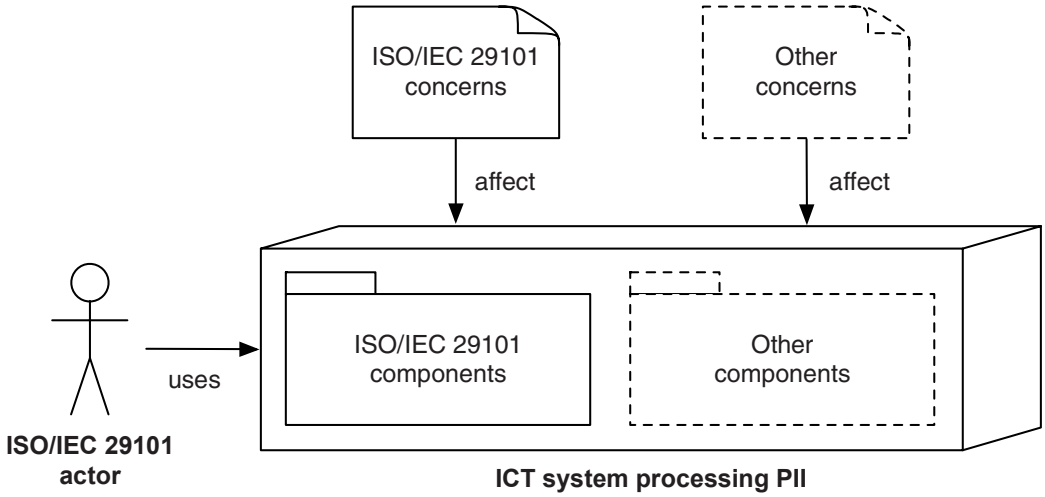

Figure 1 — Elements of the privacy architecture framework in context

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 ISO/IEC 29101 concerns and also other concerns.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

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 ISO/IEC 29101.

The ICT system may contain components from the ISO/IEC 29101 privacy architecture framework 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 standard.

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 standard.

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 standard. It is not intended as a representation of the physical structure, organisation or ownership of ICT system hardware.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

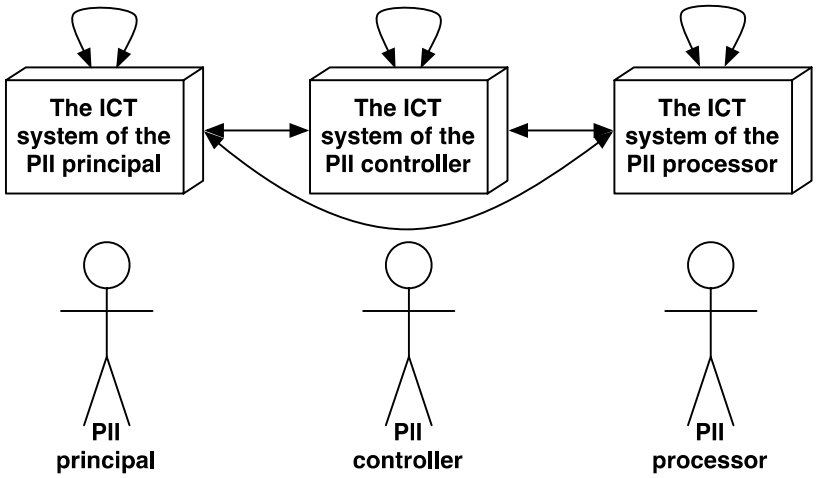

Figure 2 — The actors and their ICT systems according to ISO/IEC 29101

An actor may or may not be responsible for building the ICT systems that it uses. For example, the PII principal may use a system built by and the responsibility of the PII controller or the ICT system of the PII principal may be a part of the ICT system of the PII controller. Furthermore, the functionality of the ICT system of the PII principal might be split across different ICT hardware systems owned by the PII principal and the PII controller. Similarly, the PII controller may provide the ICT system of the PII processor. Business processes in which ICT systems are employed use a wide range of communication and trust models. The architecture framework in this international standard builds on an abstraction of these models.

If the PII principal is using a privately owned ICT system, the other privacy stakeholders may impose requirements on this ICT system. For example, the ICT system of the PII principal may have to meet a minimum baseline of security requirements to be allowed to connect to the other ICT systems. Other examples include the use of special security components like hardware authentication tokens, certain operating system versions or special web browser versions.

For example, in ICT systems employing peer-to-peer communications (communication method, communication model or communication technology featuring communication in between/among the entities that are peer to each other without central servers), every application may take the roles of all three listed actors. Information is both sent and received by each peer, so each peer could be a PII controller or processor for PII transferred by another party in the role of a PII principal.

In social networking applications, PII may be processed by anyone with access to other people's profiles. Web-based social networking applications allow all the authorized and possible anonymous users of the service to process PII provided by the PII principals connected to the social network.

6.2 Phases of the PII processing life cycle

6.2.1 Collection

Many organizations collect information from PII principals. This information can contain PII.

When collecting PII, organizations should always consider the privacy preferences and legal rights of the PII principal and privacy safeguarding requirements as stated by applicable law. Factors such as the type of PII, consent given, or any privacy preferences stated need to be considered throughout all stages of processing. PII should only be collected if it is needed for the declared purposes.

Documentation should be associated with the PII. Examples include, but are not limited to:

a. software tags that state the purpose(s) the PII can be used for;

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

b. records describing the purpose(s) that PII can be used for; and

c. records of the consent given and any specific sensitivities that should be observed (e.g., certain PII categories should be encrypted or deleted after a certain period of time).

Privacy controls should be implemented wherever data is tagged as PII or wherever PII is marked with additional information concerning the PII principal. It is also important to preserve tags that are relevant to processing PII during the usage, transfer, storage and disposal phases. If stored PII may have been modified, it should be validated for accuracy and currency before use.

In addition, PII collection processes should be designed to collect only the PII that is necessary for the respective transaction. Organizations should take steps to minimize the inadvertent/unintended collection of PII through data entry systems (e.g., web application forms that allow the entry of any information). The entry of arbitrary PII should be minimized through the use of context specific display of input fields reducing or eliminating areas in the web form where this information could be entered (e.g., removing unnecessary check boxes and free text fields). In addition, the use of fields with predefined entries (e.g., list boxes and drop-down lists), containing non-PII options, should be considered. When free form text fields are necessary, the User Interface (UI) should provide:

a. warnings to alert the PII principal not to enter PII other than that which is explicitly asked for and consented to or required by applicable law;

b. clear indication of those fields where PII is to be entered and what PII should be entered (e.g. name, address, health information); and

c. clear indication of those fields where PII should not be entered.

6.2.2 Transfer

Transferring, disseminating, or releasing PII to others means that the PII is no longer under the sole control of the PII principal. Transfer is usually the term given for dissemination of PII from the PII controller or PII processor to other PII controllers and processors. If PII is transferred from the PII controller to another actor, transfer is sometimes also referred to as disclosure.

Accountability and responsibility for the transferred PII should be agreed upon and maintained by each party involved in the PII processing. This agreement should be in writing where required by applicable law. Furthermore, such agreements will need to be compliant with data protection legislation in the source and destination domains of the transfers. When relevant and appropriate, or when legally required to do so, the PII principal should be notified that transfer is taking place and should be informed of the content and purpose of the transfer. If a dispute occurs between the PII principal and the PII controller or PII processor, records of relevant PII transfer transactions should be available to assist in resolving any such dispute.

The transfer of sensitive PII should be avoided unless it is necessary to provide a service that the PII principals has requested, it fulfils a business requirement for offering the requested service, or unless it is required by law. Some jurisdictions have instituted laws that specifically require formal contractual agreements that include all privacy safeguarding requirements between the involved parties when PII is transferred outside a jurisdiction that has a prescribed level of privacy protection. Where cross-border transfers are used, particular attention should be given to protection measures for the PII being transferred.

Appropriate protection mechanisms should be in place during the transfer of PII. In the case of a digital transfer, PII should be transmitted over a secure channel or in encrypted form if the transmission is over an insecure channel. If PII is transferred on physical media, it should be encrypted. If encryption is used, the encryption key should not be stored or transmitted together with the encrypted PII.

6.2.3 Use

Using PII means any form of PII processing that does not include “collect”, “transfer”, “store”, “archive” or “dispose”. The privacy principles described in ISO/IEC 29100 (Privacy Framework), as well as some data

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

protection and privacy laws, may limit the processing of PII if that processing is incompatible with the originally specified purposes. Therefore, PII should only be processed for the declared purposes for which it was collected.

If the PII is to be processed for any other purpose that is not covered by applicable law, consent should be obtained from the PII principal or his agent. The PII principal should be provided a means for contacting the PII controller or processor in the event there are any questions about any activities about which the PII principals is unclear.

Where such processing is considered necessary the consent of the PII principal should be obtained unless otherwise permitted by law. PII principals should be provided clear notice about the specific use of the PII.

Additionally, protection mechanisms appropriate to the usage of PII should be applied as deemed necessary by a thorough risk analysis. This includes the use of anonymization or pseudonymization techniques prior to processing and the use of secure computation techniques during processing.

6.2.4 Storage

When it is necessary to store PII, the consent of the PII principal should be obtained, taking into account any specific measures that may be required by law. In such cases, the PII should be stored only for the amount of time necessary to achieve the specific business purpose.

PII should be stored with appropriate controls and mechanisms to prevent unauthorized access, modification, destruction, removal, or other unauthorized use. Such controls include, but are not limited to, encryption, secret sharing, pseudonymization and anonymization.

Archived PII needs careful attention. The privacy principles state that PII should be retained only as long as necessary to fulfil the stated purposes and then be securely destroyed or anonymized. However, if the PII controller or PII processor is required by applicable law to retain PII after the other purposes have expired, the PII should be locked (i.e., archived and protected with an access control mechanism to prevent further usage). The primary considerations in archiving PII should be to ensure that the appropriate data protection mechanisms are in place, including access management solutions that provide access to archived PII only to authorized users.

The PII controller should implement controls in storage systems to dispose of PII when it expires or when the purpose for the storing or processing of the PII is no longer valid.

6.2.5 Disposal

In the final stage of the PII processing life cycle, PII gets deleted, anonymized, destroyed, returned or disposed of in some other way. Specific PII within PII records might get locked from unauthorized use by marking it for disposal. It should be noted that deleting PII does not necessarily mean that the PII is ultimately disposed of because PII deleted in ICT systems can often be recovered. Although it might seem to be an obvious task in PII handling, procedures concerning disposal of PII sometimes do not comply with privacy safeguarding requirements. Specifications given by the PII principal (e.g., usage purpose) or requirements specified by legislation (e.g., expiration date for specific PII) should be considered before PII is disposed of.

7 Concerns

7.1 Overview

A concern as defined in ISO/IEC/IEEE 42010 is an interest in a system relevant to one or more of its stakeholders. The privacy architecture framework in ISO/IEC 29101 focuses on concerns of the privacy stakeholders related to the processing of PII. The ISO/IEC 29101 concerns include the privacy principles of ISO/IEC 29100 and any privacy safeguarding requirements derived from and complying with these principles.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

The privacy safeguarding requirements should be determined by following a privacy risk management process complying with the process described in 4.5 of ISO/IEC 29100. Any individual or organization that is designing an ICT system that processes PII should follow this process. All the identified privacy safeguarding requirements should conform to applicable privacy legislation.

7.2 The privacy principles of ISO/IEC 29100

The PII controller is responsible for the protection of PII and the fair and lawful handling of it at all times, throughout the organization, as well as for PII processing outsourced to PII processors.

The PII controller is ultimately responsible for implementing privacy controls in an ICT system. Privacy controls are intended to ensure that the privacy safeguarding requirements set for a specific PII principal, transaction, or scenario are addressed and consistently fulfilled. Evidence of implementation should be provided by properly documenting the privacy controls that are in place and providing audit documents that verify that the controls exist, that they have been implemented correctly and that they are functioning properly. Ultimately, the PII controller should accept and adhere to the privacy principles that are described in ISO/IEC 29100.

a. consent and choice;

b. purpose legitimacy and specification;

c. collection limitation;

d. data minimization;

e. use, retention and disclosure limitation;

f. accuracy and quality;

g. openness, transparency and notice;

h. individual participation and access;

i. accountability;

j. information security; and

k. privacy compliance.

7.3 Privacy safeguarding requirements

ICT systems should implement privacy controls as a primary element in every phase of the PII processing life cycle. The privacy safeguarding requirements enable the designer of the ICT system to operationalize the link between privacy principles and the architectural components laid down in Clause 8.

In order to implement effective privacy controls in an ICT system, PII processing flows describing the PII processing should be created. PII processing flow diagrams are a graphical representation of the “flow” of PII through the ICT system and between the different actors. For example, if an actor transfers PII to other actors (e.g., PII processors) the PII processing flow diagram should include those PII transfers.

A PII processing flow diagram may also be represented as a PII flow table. This diagram or table follows the collection, transfer, use, storage or disposal of PII and includes information such as the type of PII, who collected the PII, the purpose for processing, to whom the PII is going to be transferred, the receipt of consent by the PII principal, the retention period and at which location it will be stored and the resulting privacy risk level. The PII processing flow information will be an input to the privacy risk management process that outputs the privacy safeguarding requirements.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

After the requirements analysis of an ICT system has been completed, the developers should cross-reference the privacy safeguarding requirements of the ICT system with the list of concerns in this standard. The privacy safeguarding requirements should then be used for choosing the architectural components that satisfy said requirements.

Annex A of this international standard contains an example list of concerns and illustrates how to link concerns to the privacy principles of ISO/IEC 29100 and the architectural components of ISO/IEC 29101.

8 Architectural views

8.1 Introduction

The architectural views in this clause are structured into three views. First, the component view describes the ICT system components in detail and separates them into layers based on their functionality. Each layer groups components that help to contribute to the proper processing of PII. Limited implementation guidance is given for each component. Actor-specific guidance is given where applicable. This view is helpful for understanding the building blocks in the privacy architecture framework.

Tables showing examples of typical relationships between the privacy principles of ISO/IEC 29100 and the components of the architecture are provided in the component view. Such mapping tables are helpful for understanding how an ICT system adheres to the privacy principles of ISO/IEC 29100. Similar tables could be used as examples and updated during system design to describe how a particular ICT system adheres to the privacy principles in ISO/IEC 29100.

The actor view looks at the components described in the component view from the perspective of the ICT system of an individual actor. This view is helpful in the design of the architecture of a particular ICT system. The interaction view looks at the components from a deployment perspective. This view is helpful for understanding how components in the ICT systems of different actors interact with each other.

8.2 Component view

The component view is meant to describe ICT system components that are involved in the processing of PII.

The choice of components should be guided by the appropriate privacy safeguarding requirements. The developer of the ICT system for a specific actor(s) (see Figure 2) should use the component view to determine the components that need to be included in the architecture of the system that they are developing. This architecture should be based on the privacy safeguarding requirements established using the guidance given in Clause 7. Note that not all components described in this international standard will necessarily be appropriate in a particular ICT system.

The component view is presented in three layers. Each layer is a logical group of components that contribute to a specific goal in the processing of PII. Components in the privacy settings layer handle the management of metadata about PII processing including, among others, the exchange of information on the purpose of processing, consent and preferences of the PII principal. Components in the identity and access management layer are responsible for ensuring that proper identity information is used in PII processing and access to the PII is controlled according to the privacy safeguarding requirements. Finally, components in the PII layer perform various tasks to process the PII.

The architecture framework is designed with the assumption that all components interact with several other components. However, in order to maintain generality and readability, the possible interactions between components have been omitted from the representation.

Some of the components in the architecture framework are Privacy Enhancing Technologies (PETs). This selection of PETs is not comprehensive. There exist other PETs that are not described within this standard and the developer of the ICT system is responsible for choosing appropriate PETs and adapting them to this architecture framework.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

Annex B of this international standard gives an example of an ICT system architecture that applies PETs for securely processing PII. Annex C of this international standard gives an example of how to use attribute-based credentials to build an ICT system that provides pseudonymous identity and access control management.

The following sections describe the layers, the components within them and the actors that interact with the components. A general description of each component is given and it is followed by actor-specific guidelines. For some components, no guidance specific to the ICT systems of a particular actor is given, as the behaviour of the component is similar in the ICT systems of all actors.

8.2.1 Privacy settings layer

The privacy settings layer comprises components that communicate the system privacy policy to the relevant actors and implement the system privacy safeguarding requirements. These components let the ICT system communicate the system privacy policy and implement the corresponding privacy safeguarding measures.

In addition, the components in this layer should convey to the PII controller and PII processor any privacy preferences and consent information that have been collected from the PII principal.

8.2.1.1 Policy and purpose communication

General. This component is responsible for relaying information, including updates, about the privacy policy of the PII controller and the purpose of PII collection to the ICT systems of privacy stakeholders.

The communicated information should contain at least the following:

a. the identities of the PII controllers and any associated PII processors;

b. policies regarding the transfer of PII to PII processors;

c. the use of privacy enhancing technologies (such as anonymization) with their respective goals;

d. the purposes for which the PII is collected;

e. identification of the PII to be collected; and

f. the legal rights of the PII principal to access their PII to determine the extent of the PII stored and to check for and correct any inaccuracies, and the procedures for doing so.

PII principal. The policy and purpose communication component of the ICT system of the PII principal should:

a. receive policy and purpose information from the corresponding component in the ICT system of the PII controller;

b. interpret the received information and display or otherwise convey to the PII principal in a clearly comprehensible manner its meaning;

c. offer the PII principal the opportunity to locally store the received information; and

d. confirm to the PII controller that the policy and purpose information has been received by the PII principal.

PII controller. The policy and purpose communication component of an ICT system under the control of the PII controller should:

a. store policy and purpose information that has been conveyed to PII principals;

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013

b. log the acts of conveying policy and purpose information to PII principals in such a way that it can be established which information was current and was conveyed to PII principals at which time, along with confirmation of receipt of this information;

c. convey the current policy and purpose information to the corresponding component of the ICT system of the PII principal in such a manner that it can be used by this system directly to inform the PII principal in a complete and comprehensible manner, or that it can be mapped by said component to such a form by some pre-defined mapping;

d. convey a reference to the displayed policy and purpose information to those components which handle the storage of consent information and storage of PII itself; and

e. transmit updates about changes to policy and purpose information to the corresponding components of the ICT systems belonging to those PII principals who have consented to receive such information.

PII processor. The ICT system of the PII processor typically should receive digital copies of the privacy policy and the processing purpose from the ICT system of the PII controller. The ICT system of the PII processor should present the privacy policy and processing purpose documentation received from the PII controller in a clearly comprehensible form to everyone with access to PII governed by that policy.

The PII controller may arrange the processing of PII by various PII processors. The purpose communication component in the ICT system of the PII controller should transmit the purpose associated with the PII provided to all relevant PII processors. Each PII processor should be informed of the purpose(s) for processing the PII.

8.2.1.2 PII categorization

General. An ICT system processing PII has to be aware of the categories of PII that it processes so that it can distinguish between different types of data (e.g., sensitive PII, PII and non-PII). This is necessary for services processing PII differently depending on category. Additionally, the ICT system should be aware of PII values that contain direct identifiers such as names and social security numbers. This component should implement the functions that provide such a categorization in the ICT system.

When dealing with non-PII, the risk of combining non-PII to infer or derive an identity or profile of a unique user or at least small enough subset of users should be understood and evaluated.

All PII should be categorized correctly in order that it is processed and stored by the ICT system in accordance with its marked sensitivity. If PII has been unknowingly collected, e.g. as a result of unsolicited input, it may not be possible to do this and measures should therefore be taken to minimise the possibility of unsolicited PII collection.

While the ICT system should be aware of PII values that contain direct identifiers such as names and social security numbers, it may not be possible to do this if unsolicited PII has been collected.

PII principal. The ICT system of the PII principal should be capable of identifying the categorization marking associated with the PII and should process the PII in accordance with its category. The categorisation can also be used to identify the PII that should be protected using PETs (e.g. sensitive PII). The PII categorization component also provides further categorization of the PII into sub-categories where sub-categories are a requirement of a specific application domain.

PII controller. The ICT system of the PII controller should contain a comprehensive categorization of PII used in the ICT systems processing the categorized PII. This information should be transmitted to PII processors. Also, this categorization can be used by the audit logging, PII pseudonymization, PII disclosure and PII archiving and retention components so they can determine which parts of the data contain PII.

PII processor. The ICT system of the PII processor should be capable of processing the PII categorization associated with the received PII. The information should be used in PII auditing and secure PII processing.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29101:2013