ISO/IEC 29101:2018 (E)

Information technology — Security techniques — Privacy architecture framework

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviated terms

5 Overview of the privacy architecture framework

5.1 Elements of the framework
5.2 Relationship with management systems

6 Actors and PII

6.1 Overview
6.2 Phases of the PII processing life cycle
6.2.1 Collection
6.2.2 Transfer
6.2.3 Use
6.2.4 Storage
6.2.5 Disposal

7 Concerns

7.1 Overview
7.2 The privacy principles of ISO/IEC 29100
7.3 Privacy safeguarding requirements

8 Architectural views

8.1 General
8.2 Component view
8.2.1 General
8.2.2 Privacy settings layer
8.2.2.1 General
8.2.2.2 Policy and purpose communication
8.2.2.3 PII categorization
8.2.2.4 Consent management
8.2.2.5 Privacy preference management
8.2.2.6 Relationship between privacy principles and components in the privacy settings layer
8.2.3 Identity management and access management layer
8.2.3.1 General
8.2.3.2 Identity management system
8.2.3.3 Pseudonymization scheme
8.2.3.4 Access control
8.2.3.5 Authentication
8.2.3.6 Authorization
8.2.3.7 Relationship between privacy principles and components in the identity and access management layer
8.2.4 PII layer
8.2.4.1 PII management
8.2.4.2 PII transfer

8.2.4.3 PII validation
8.2.4.4 PII pseudonymization
8.2.4.5 PII anonymization
8.2.4.6 Secret sharing
8.2.4.7 PII encryption
8.2.4.8 PII use
8.2.4.9 Secure computation
8.2.4.10 Query management
8.2.4.11 PII inventory
8.2.4.12 PII disclosure
8.2.4.13 PII archiving and retention
8.2.4.14 Audit logging
8.2.4.15 Relationship between privacy principles and the components in the PII layer
8.3 Actor view
8.3.1 General
8.3.2 ICT system of the PII principal
8.3.3 ICT system of the PII controller
8.3.4 ICT system of the PII processor
8.4 Interaction view
8.4.1 General
8.4.2 Privacy settings layer
8.4.3 Identity and access management layer
8.4.4 PII layer

Annex A (informative) Examples of the PII-related concerns of an ICT system

A.1 General
A.2 Obtaining and communicating consent
A.3 Communicating the purpose of PII collection
A.4 Secure PII processing
A.5 Classification and control of PII
A.6 Accounting and Audit of PII operations
A.7 Archiving and disposal of PII
A.8 Relationship with privacy principles

Annex B (informative) A PII aggregation system with secure computation

B.1 General
B.2 Purpose, actors and deployment
B.3 Architecture for the PII entry application
B.4 Architecture for the study control application
B.5 Architecture for the secure PII analysis application
B.6 Conclusion

Annex C (informative) A privacy-friendly, pseudonymous system for identity and access control management

C.1 General
C.2 Purpose, actors and deployment
C.3 Architecture of the ICT system of the University Credential Issuer
C.4 Architecture of the ICT system of the student
C.5 Architecture of the Course Evaluation Application
C.6 Conclusion

Page count: 42