

ISO/IEC 29101:2013-10 (E)

Information technology - Security techniques - Privacy architecture framework

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
7.3	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 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