

ISO/IEC 24760-2:2025-09 (E)

Information security, cybersecurity and privacy protection - A framework for identity management - Part 2: Reference architecture and requirements

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	3
5	Reference architecture	3
5.1	General	3
5.2	Deployment scenarios	3
5.3	Stakeholders	4
5.3.1	General	4
5.3.2	Principal	5
5.3.3	Identity management authority	5
5.3.4	Identity information authority	6
5.3.5	Relying party	6
5.3.6	Regulatory body	6
5.3.7	Consumer/citizen representative or advocate	6
5.4	Actors	7
5.4.1	General	7
5.4.2	Principal	8
5.4.3	Identity management authority	8
5.4.4	Identity registration authority	9
5.4.5	Relying party	10
5.4.6	Identity information authority	10
5.4.7	Identity information provider	11
5.4.8	Verifier	12
5.4.9	Auditor	13
5.5	Processes and services	13
5.5.1	Documentation	13
5.5.2	Identity information management processes	14
5.5.3	Specific identity information management processes	15
5.5.4	Additional functions	17
5.6	Viewpoints	20
5.6.1	General	20
5.6.2	Context viewpoint	20
5.6.3	Functional viewpoint	20
5.7	Use cases	21
5.7.1	General	21
5.7.2	Principal use cases	22
5.8	Components	23
5.8.1	General	23
5.8.2	Principal	23
5.8.3	Identity register	23
5.9	Compliance and governance	24
5.10	Physical model	24

6	Architecture for managing internal identities, the enterprise model	24
6.1	Context	24
6.2	Stakeholders and concerns	25
6.3	The enterprise deployment scenario	26
6.4	Use cases	26
6.4.1	Employee use cases	26
6.4.2	Employer use cases	27
7	Architecture for managing external identities	27
7.1	Context	27
7.2	Stakeholders and concerns	27
7.3	Deployment scenarios with external identities	29
7.3.1	The federated deployment scenario	29
7.3.2	The service deployment scenario	29
7.3.3	The federated deployment scenario as applied as a service	29
7.4	Use cases	29
7.4.1	Device use cases	29
7.4.2	Sharing use cases	29
8	Requirements for the management of identity information	30
8.1	General	30
8.2	Access policy for identity information	30
8.3	Functional requirements for management of identity information	30
8.3.1	Policy for identity information lifecycle	30
8.3.2	Conditions and procedure to maintain identity information	31
8.3.3	Identity information interface	31
8.3.4	Reference identifier	31
8.3.5	Identity information quality and compliance	33
8.3.6	Archiving information	33
8.3.7	Terminating and deleting identity information	33
8.4	Non-functional requirements	34
	Annex A (informative) Use case	35
	Annex B (informative) Component model	38
	Annex C (informative) Business process model	41
	Bibliography	46