

ISO/IEC 27566-1:2025-12 (E)

Information security, cybersecurity and privacy protection - Age assurance systems - Part 1: Framework

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
3.1	Terms relating to age assurance	1
3.2	Terms relating to actors and parties	3
3.3	Terms relating to data and processes	4
4	Overview of age assurance	7
4.1	Age	7
4.2	Characteristics of age assurance systems	7
4.3	Age assurance methods	8
4.3.1	Overview of age assurance methods	8
4.3.2	Age verification methods	8
4.3.3	Age estimation methods	9
4.3.4	Age inference methods	10
4.3.5	Successive validation	10
4.4	Stakeholders	10
4.4.1	General	10
4.4.2	Policy makers	10
4.4.3	Consumer protection agencies	11
4.4.4	Sector associations	11
5	Functional characteristics	11
5.1	Age assurance systems	11
5.1.1	General	11
5.1.2	Age assurance providers	11
5.1.3	Intermediaries	12
5.2	Data acquisition for age assurance components	12
5.2.1	Sources of data	12
5.2.2	Primary and secondary credentials	12
5.2.3	Date transposition errors	13
5.3	Binding of age assurance result to the correct individual	13
5.3.1	Binding characteristics	13
5.3.2	Approaches to binding	13
5.4	Age assurance data processing	14
5.5	Configuration management	14
5.6	Context in use	15
5.7	Delivery of age assurance result	15
6	Performance characteristics	15
6.1	Performance effectiveness	15
6.1.1	General	15
6.1.2	Effective age assurance systems	15
6.1.3	Ineffective age assurance systems	16
6.1.4	Use of self-asserted age	16

6.1.5	Other factors affecting effectiveness	16
6.2	Indicators of effectiveness	16
6.3	Performance metrics	17
6.3.1	Classification accuracy	17
6.3.2	Primary metrics	17
6.3.3	Outcome error parity	17
6.3.4	Performance efficiency	17
6.4	Resource utilization	18
6.5	Testability	18
7	Privacy characteristics	18
7.1	General	18
7.2	Privacy by design and default	18
7.3	Data minimization	19
7.3.1	Collection limitation	19
7.3.2	Non-disclosure of age-related data	19
7.3.3	Compliance with legal obligations	19
7.3.4	Purpose limitation	19
7.3.5	Access control	19
7.3.6	Data disposal	19
7.4	Avoidance of adding to digital footprint	19
7.5	User awareness	20
7.6	Audit logs	20
8	Security characteristics	21
8.1	Security by design and default	21
8.2	Replay, forwarding or reuse of age assurance result	21
8.2.1	Replay of an age assurance result	21
8.2.2	Forwarding of an age assurance result	21
8.2.3	Planned memorization or reuse of an age assurance result	21
8.3	Resistance to attack	22
8.3.1	Preparation for attack	22
8.3.2	Attack vectors	22
8.3.3	Biometric presentation attacks	22
8.3.4	Spoofing attack	23
8.3.5	Counterfeiting attack	23
8.4	Contra indicators	23
8.5	Fail safe	23
9	Acceptability characteristics	24
9.1	General	24
9.2	Inclusivity	24
9.3	User engagement and assistance	24
9.4	Complaint handling	25
10	Practice statements	25
10.1	General	25
10.2	Practice statements by age assurance providers	26
10.3	Practice statements by relying parties	27
10.4	Practice statements by intermediaries	28
	Bibliography	29