

ISO/IEC 27551:2021-09 (E)

Information security, cybersecurity and privacy protection - Requirements for attribute-based unlinkable entity authentication

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	2
5	General objectives of attribute-based entity authentication	2
6	Properties of attribute-based entity authentication protocols	4
6.1	Correctness	4
6.2	Unforgeability	4
6.2.1	General	4
6.2.2	Replay protections	4
7	Unlinkability properties of attribute-based entity authentication protocols	4
7.1	General	4
7.2	Generic definition of unlinkability	5
7.3	Specific definitions of unlinkability	5
7.3.1	General	5
7.3.2	Passive outsider unlinkability (anti-tracking from passive outsiders)	7
7.3.3	Active outsider unlinkability (anti-tracking from active outsiders)	7
7.3.4	RP-U unlinkability ("anonymous visits" to an RP)	7
7.3.5	AP-U unlinkability	8
7.3.6	RP+AP-U unlinkability (anti-RP-AP-collusion)	8
7.3.7	AP-RP unlinkability (anti-tracking of RP from AP)	8
7.3.8	AP-RP+U unlinkability	8
7.3.9	RP+RP'-U unlinkability (anti-tracking of U from a set of colluding RPs)	8
7.4	Relationships between notions of unlinkability	9
7.5	Unlinkability levels for attribute-based entity authentication	9
7.6	Models	10
8	Attributes	10
8.1	Categories of attributes	10
8.1.1	Personal attributes	10
8.1.2	Self-claimed attributes	10
8.1.3	Verified attributes	10
8.1.4	Static attributes	11
8.1.5	Semi-static attributes	11
8.1.6	Dynamic attributes	11
8.1.7	Computed attributes	11
8.1.8	Identifying attributes	11
8.1.9	Supporting attributes	11
8.2	Verified attribute expiry and revocation	11
8.3	Attribute assurance	11

9	Requirements for level N attribute-based unlinkable entity authentication	11
	Annex A (informative) Formal definitions for security and unlinkability notions	13
	Annex B (informative) Examples of attribute-based entity authentication protocols	19
	Annex C (informative)	26
	Annex D (informative) Use cases for attribute-based unlinkable entity authentication	33
	Bibliography	34