

# ISO 22378:2022-12 (E)

## Security and resilience - Authenticity, integrity and trust for products and documents - Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Abbreviated terms .....	2
5	Overview .....	2
5.1	General .....	2
5.2	Object identification systems -- Operating process .....	3
5.2.1	General .....	3
5.2.2	Object examination function .....	3
5.2.3	Trusted query processing function .....	4
5.2.4	Trusted verification function .....	4
5.2.5	Attribute data management system .....	4
5.2.6	Response formatting function .....	4
5.3	Object identification systems -- Set-up of trusted framework .....	4
5.3.1	General .....	4
5.3.2	Owner .....	5
5.3.3	UID-generating function .....	5
5.3.4	Object information .....	5
5.3.5	UID verification rules .....	6
5.3.6	Physical identity assignment .....	6
5.3.7	Object attribute data .....	6
5.3.8	Data management rules .....	6
5.3.9	Query processing rules .....	6
6	Key principals .....	6
6.1	General .....	6
6.2	Availability and timely response .....	6
6.3	One authoritative source .....	7
6.4	Data management .....	7
6.5	Need to know .....	7
6.6	Data protection .....	7
6.7	Privacy .....	7
6.8	Regulatory compliance .....	8
6.9	Vetting .....	8
6.10	Interoperability aspects .....	8
6.11	UID generation .....	8
7	Plan and implementation .....	9
7.1	General .....	9
7.2	Determination of trusted services .....	9
7.2.1	General .....	9

7.2.2	Trust in the TQPF .....	9
7.2.3	Use of prefix or postfix .....	9
7.2.4	Object examination techniques .....	9
7.3	Management of object identification data and attributes .....	10
7.3.1	General .....	10
7.3.2	Verify the service entry point (TQPF) .....	10
7.3.3	Maintenance and management .....	10
7.3.4	Privilege levels and user roles .....	10
7.3.5	Access control .....	10
7.3.6	Ownership of transactional data .....	11
7.3.7	Use of transactional data .....	11
7.3.8	Governmental or intergovernmental agencies or competent authorities .....	11
7.4	Common frauds .....	11
7.4.1	Duplicate UID codes .....	11
7.4.2	Substitution .....	12
7.4.3	Feature deception .....	12
7.4.4	Malicious services .....	13
7.4.5	Malicious inspector .....	13
7.4.6	Insider attacks .....	13
Annex A (informative) Digital certificate (for inspectors) .....		15
Annex B (informative) Master data management .....		18
Annex C (informative) Illustrative implementation examples .....		19
Bibliography .....		24