

ISO 22381:2018 (E)

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for establishing interoperability among object identification systems to deter counterfeiting and illicit trade

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Abbreviated terms
5	Planning, implementing and controlling systems' interoperability
5.1	Identify stakeholders and their needs
5.2	Organize stakeholders
5.2.1	Identify lead stakeholder
5.2.2	Define roles and responsibilities
5.2.3	Develop a contractual framework
5.2.4	Set up an onboarding and leaving process
5.3	Plan architecture
5.3.1	General principles
5.3.2	Identify participating OIAs and functional blocs to form the constituents of the I-OP
5.3.3	Study types and ownership of attributes to be handled
5.3.4	Specify TEPs for secure I-OP access
5.3.5	Specify access rules for users
5.3.6	Define and improve trust levels
5.3.7	Outline or delimit the usage of participating OIAs and their functional units
5.3.8	Draft an I-OP architecture
5.3.9	Return information back to the source
5.4	Plan and implement operations
5.4.1	Define data exchange formats
5.4.2	Establish trust into the service behind a particular UID
5.4.3	Delimit data inputs and outputs
5.4.4	Define storage and custodianship of data inputs and outputs
5.4.5	Define operational responsibilities
5.4.6	Prepare for systems failures
5.4.7	Negotiate alarm responses of common interest
5.4.8	Run pilots
5.5	Review and improve
5.5.1	General
5.5.2	Revisit stakeholders' expectations
5.5.3	Review operations
5.5.4	Review security
5.5.5	Review technology
Annex A	(informative) Typical stakeholder interests in an I-OP
Annex B	(informative) The role of trusted entry points for user groups
Annex C	(informative) Types of information exchanged in I-OP architectures
C.1	Free use of non-structured and not predefined information
C.2	Information exchange using predefined formats and content