

ISO/TR 24371:2025-09 (E)

Financial services - Natural person identifier (NPI) - Natural person identifier lifecycle operation and management

Contents		Page
Foreword		vi
Introduction		vii
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	8
5	NPI standard: ISO 24366	10
6	Overview of requirements	10
6.1	Introduction	10
6.2	Business requirements	10
6.3	Functional requirements	11
7	Risk and risk mitigation considerations	11
7.1	General	11
7.1.1	Major types of risk	11
7.1.2	Compliance risk	11
7.1.3	Complexity risk	12
7.1.4	IT/cybersecurity risk	12
7.1.5	Fraud risk	12
7.1.6	Identity management risks	12
7.1.7	Data quality risk	12
7.1.8	Opportunity risk	12
7.1.9	Branding/reputation risk	13
7.2	Scope of use and liability	13
7.3	Risk mitigation policies	13
7.4	Risk mitigation strategy	13
7.4.1	General	13
7.4.2	Identify	14
7.4.3	Protect	15
7.4.4	Detect	15
7.4.5	Respond	15
7.4.6	Recover	16
8	Policy considerations	16
8.1	Major policy considerations	16
8.1.1	General	16
8.1.2	Uniqueness	16
8.1.3	Scale	17
8.1.4	Performance	17
8.1.5	Extensibility	18
8.1.6	Interoperability	18
8.1.7	Realisation of potential benefits	18
8.2	Outline process: NPI lifecycle	18
8.3	User journey	20

8.4	Main actors in the NPI lifecycle	20
8.4.1	General	20
8.4.2	Actor enrolment	21
9	Framework considerations: Entity Authentication Assurance Framework	22
9.1	General	22
9.2	Phase 1: Enrolment	23
9.2.1	General	23
9.2.2	Application	24
9.2.3	Identity proofing	24
9.2.4	Evidence of identity	25
9.2.5	Process flow	26
9.2.6	Identity-person binding	28
9.2.7	Biometrics	28
9.3	Phase 2: Provisioning and issuance	29
9.3.1	General	29
9.3.2	Account creation	29
9.3.3	NPI creation	29
9.3.4	NPI issuance	29
9.4	Phase 3: Use	30
9.4.1	NPI holder	30
9.4.2	Relying parties	30
9.4.3	NPI authorised entities	30
9.4.4	NPI issuer	31
9.4.5	Links to other identifiers	32
9.5	Phase 4: Management of the NPI lifecycle	32
9.5.1	General	32
9.5.2	Suspension	32
9.5.3	Restoration	32
9.5.4	Revocation	33
10	NPI issuer operational considerations	33
10.1	General	33
10.2	Responsibility	33
10.3	NPI community architecture	33
10.4	Sizing and performance	33
10.4.1	General	33
10.4.2	Global NPI sizing	34
10.4.3	Sizing for one NPI register	34
10.4.4	Global NPI policy	34
10.4.5	Policy for an NPI register	34
10.4.6	Access control	35
10.4.7	Virtual NPI	35
10.4.8	Maintenance operations	36
10.5	Relying party operations	36
11	Technology considerations	36
11.1	General	36
11.2	NPI privacy preservation	37
11.2.1	Privacy impact assessment	37
11.2.2	Privacy preservation techniques	37
11.3	NPI data security operations	37
11.4	Counter-fraud: Monitoring and anomaly detection	37
11.5	Cybersecurity	37
12	NPI governance	38
12.1	General	38
12.2	General governance principles	38
12.3	Evolving discussions and future directions in NPI governance	39
12.4	Inter-registry operations	39
12.5	Relying party operations	40

12.6	NPI community	40
12.7	Federation	40
12.8	NPI governance structure	41
12.8.1	General	41
12.8.2	NPI issuers	41
Annex A (informative) NPI background		43
Annex B (informative) Customer due diligence and enhanced due diligence		45
Annex C (informative) Cybersecurity considerations		47
ISO/TR 24371:2025(en) Annex D (informative) Biometric considerations		52
Annex E (informative) NPI data quality management considerations		61
Annex F (informative) International organizations: the World Bank and the Organization for Economic Co-operation and Development (OECD)		63
Annex G (informative) NPI register operations: Challenges and best practices		66
Annex H (informative) Aadhaar		74
Annex I (informative) Use cases		79
Annex J (informative) Business case for the NPI		92
Annex K (informative) Overview of key documents		95
Bibliography		97