



BSI Standards Publication

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

National foreword

This Published Document is the UK implementation of ISO/TR 24371:2025.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 28321 1

ICS 03.060

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 September 2025.

Amendments/corrigenda issued since publication

Date	Text affected



Technical Report

ISO/TR 24371

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

*Services financiers — Identifiant de personne physique —
Fonctionnement et gestion du cycle de vie de l'identifiant de la
personne physique*

**First edition
2025-09**



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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

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

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of patents which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 8, *Reference data for financial services*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The regulatory, business and consumer requirements to identify natural persons for the purposes of provision of an expanding range of digital financial services are rapidly increasing, nationally and internationally. However, the abuse, misuse and criminal exploitation of personal data are also rising significantly, facilitated by uncontrolled data proliferation and data sharing that is contrary to privacy regulations and societal norms. Risks and tangible harms to people and organizations, and to our digital economies and societies, are growing as a direct consequence. There are increasing requirements for consumer protection.

Protecting the personal data of employees of financial services firms and of natural persons as customers of financial and non-financial firms is important. This protection allows these firms to respond to regulatory requirements without exposing personal information. It also provides regulators with a privacy-protected way to identify all parties involved. This is crucial for the safe and conformant management of financial assets at rest and in transit. This is particularly important in areas such as payments, cards, securities, trading and crypto asset systems.

One of the biggest problems is the lack of a globally acceptable identifier for a natural person to enable cross-organizational and cross-border financial processes to operate safely and with regulatory compliance. This would provide the organizations involved with a common reference point for the purposes of validating an identity but without unauthorised sharing or exposing personal data as part of the financial transaction.

The natural person identifier (NPI) is this global identifier, and its format is specified in ISO 24366. The NPI supports many identifications, know your customer and traceability use cases, including persons of significant control and beneficial owners. It can also support new safe and regulatory conformant implementations of digital money, such as digital cash, central bank digital currencies (CBDCs), currency trading and digital asset trading.

The NPI is primarily for financial purposes within and across legal, registered organizations. However, its use is not limited to financial institutions or purposes. In practice, this includes almost all industry and government organizations.

Benefits include:

- reducing costs and risks in straight-through processes;
- reducing friction and creating velocity in payment systems;
- enabling better monitoring of systemic risk across jurisdictions, particularly to reduce fraud and financial crime;
- greater protection of citizens' personal information during the provision of services;
- improving measurable regulatory compliance;
- enabling better evidence for more successful investigations and prosecutions.

This document describes the needs of the global financial services industry and the regulatory community for natural person identification in order to create NPI standards for implementation and operation. Emerging key provisions are that such NPI standard(s):

- enable unique identification globally of natural persons requiring an identifier;
- support cross-border payment, card, trading and securities processes;
- enable interoperability and co-existence between national identifiers and the international NPI;
- define an NPI that contains no embedded intelligence;
- define an NPI that is interoperable with other standards and existing reference data and can be applied globally to support the financial services industry;

- address interoperability of existing natural person identifiers (e.g. national security number, social security number, national insurance number, tax identification number, national ID) and the globally applicable NPI;
- describe normative methods and procedures for authentication, identification and issuance;
- give guidance;
- define governance for the issuance and maintenance of NPIs, in a privacy protected way;
- leverage expertise in defining and maintaining identifier standards;
- define an NPI scheme that is reliable and an NPI that is persistent;
- define an NPI schema that is extensible and free from limitation on use and redistribution;
- can be linked to a verifiable legal entity identifier (vLEI) role for a legal person belonging to a legal entity organization with a LEI.

Further background information is provided in [Annex A](#). A business case for the NPI is provided in [Annex I](#). An overview of key documents is provided in [Annex K](#).

ISO 24366 provides the syntax and a comprehensive list of reference data attributes to identify the natural person uniquely to any financial organization or organization involved in financial processes.

Key factors affecting any considerations regarding the future success of the NPI include the following:

- The justification for the NPI remains strong and is growing. Its potential contribution to some UN Sustainability Development Goals and programmes is recognised.
- The number of interested national and international parties is significant and continues to grow quickly, but the situation is fragmented and there is no clear stakeholder community or collaborative convening body. However, there is a growing desire to collaborate amongst many major and international organizations.
- The NPI has the potential to address many privacy-preserving identification, compliance and traceability risks and requirements in financial services, particularly in cross-border situations. However, the benefits go much wider. It has the potential to address many other risks and requirements across regulated industries and government services, and to assist in the fight against financial crime.
- The NPI can become an important interoperability mechanism, acting as a connector between national digital ID systems that operate at high assurance according to international standards.
- The many benefits assist in increasing financial, digital and social inclusion within countries that have growing digital economies and societies, which helps developing countries to accelerate their digital maturity and inclusion.
- This document contains enough information and knowledge to inform a series of practical next steps to implement ISO 24366, to operate and to deliver a series of first order and second order benefits.
- Action is required as soon as possible to ensure that the current NPI community of interest can continue to work without interruption. The greatest concern amongst those investing in the NPI's progress is that it will stall due to bureaucratic delays that are incompatible with the pace of digitisation.
- This document provides a concise body of knowledge for regulators, stakeholders and participants and to de-risk subsequent operational and counter-fraud implementations.
- Furthermore, a top-level regulatory and strategic mandate with an operational governance model to match, similar to ICANN and the Global LEI Foundation (and its Regulatory Oversight Committee) is considered fundamentally important to build the NPI community of stakeholders and shape the global governance body – this would happen outside ISO. Organizations in TC 68, *Financial services*, and elsewhere, particularly regulators and authorities, also seek to follow a similar approach to that which created the LEI's operational governance model and its top-level mandate from the G20 and key

international organizations, including the FSB and FATF. This would accelerate progress, maximise re-use and enable synergies and interoperability.

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

1 Scope

This document provides an overview of regulatory, business and best practice risk mitigation specifications that apply to the implementation, operation and governance of natural person identifier (NPI) policies, procedures and mechanisms necessary to support the lifecycle of all NPIs.

The purpose of this document is to provide the basis for the development of one or more international standards related to the safe creation, use and management of NPIs with maximum global interoperability.

For the structure of the NPI, see ISO 24366. For reference, ISO 24366 specifies a machine-readable, unambiguous NPI and the relevant reference data to uniquely identify the natural person relevant to any financial transaction rather than the personal identifying information.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 authentication

provision of assurance in the identity of an entity

[SOURCE: ISO/IEC 29115:2013, 3.2].

3.2 authentication factor

piece of information and/or process used to authenticate or verify the identity of an entity

Note 1 to entry: Authentication factors are divided into four categories:

- something an entity has (e.g. device signature, passport, hardware device containing a credential, private key).
- something an entity knows [e.g. password, personal identification number (PIN)];
- something an entity is (e.g. biometric characteristic);
- something an entity typically does (e.g. behaviour pattern).

[SOURCE: ISO/IEC 29115:2013, 3.3]

3.3

authentication protocol

defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity

[SOURCE: ISO/IEC 29115:2013, 3.4]

3.4

authenticator

something the subject possesses and controls that is used to authenticate the subject's identity

Note 1 to entry: An authenticator can be data in the form of a credential or an algorithm to process a challenge or response, secured in software or a hardware device.

3.5

authoritative source

repository which is recognized as being an accurate and up-to-date source of information

Note 1 to entry: The authority is normally legally binding under statute or contract law.

[SOURCE: ISO/IEC 29115:2013, 3.5, modified – Note 1 to entry was added.]

3.6

biometric identification

process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual

[SOURCE: ISO/IEC 30108-1:2015, 4.6]

3.7

claim

statement that something is the case, without being able to give proof

Note 1 to entry: The meanings of the terms "claim" and "assertion" are generally agreed to be similar but slightly different. For the purposes of this document, an assertion is considered to be a stronger statement than a claim, because it is based on evidence or proof, whereas a claim is not.

[SOURCE: ITU-T X.1252: 04/2021, 6.19]

3.8

context

environment with defined boundary conditions in which entities exist and interact

[SOURCE: ITU-T X.1252: 04/2021, 6.22]

3.9

corroborative source

data source that is not legally authoritative

3.10

credential

set of data presented as evidence of a claimed or asserted identity and/or entitlements

Note 1 to entry: See ISO/IEC 29115:2013, Annex B for additional characteristics of a credential.

[SOURCE: ISO/IEC 29115:2013, 3.8]

3.11

credential service provider

trusted actor that issues and/or manages credentials

[SOURCE: ISO/IEC 29115:2013, 3.9]

3.12

data protection

implementation of appropriate administrative, technical or physical means to guard against unauthorised intentional or accidental disclosure, modification or destruction of data

3.13

enrolment

process to make an entity known within a particular domain

Note 1 to entry: Enrolment typically comprises the collection and validation of identity information for identification of an entity and the collection of the identity information required for identity registration, followed by identity registration itself.

[SOURCE: ISO/IEC 24760-1:2019, 3.4.3]

3.14

entity

something that has separate and distinct existence and that can be identified in a context

Note 1 to entry: For the purposes of this document, entity is also used in the specific case for something that is claiming an identity.

[SOURCE: ITU-T X.1252: 04/2021, 6.33]

3.15

entity authentication assurance

degree of confidence reached in the authentication process that the entity is what it is, or is expected to be

Note 1 to entry: The confidence is based on the degree of confidence in the binding between the entity and the identity that is presented.

Note 2 to entry: This definition is based on that of authentication assurance given in b-ITU-T X.1252.

3.16

global NPI authority

GNPIA

global authority for the conformant operation of all natural person identifier (NPI) registers

Note 1 to entry: The GNPIA is subordinate to the NPI governance body.

3.17

identifier

one or more attributes that uniquely characterize an entity in a specific context

[SOURCE: ISO/IEC 29115:2013, 3.12]

3.18

identity

set of attributes related to an entity

Note 1 to entry: Within a particular context, an identity can have one or more identifiers to allow an entity to be uniquely recognized within that context.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.2, modified - Notes 1 to 3 to entry from the original document were replaced with Note 1 to entry]

3.19

identity information verification

process of checking identity information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness and binding to the entity

[SOURCE: ISO/IEC 29115:2013, 3.14]

3.20

identity proofing

process by which the registration authority captures and verifies sufficient information to identify an entity to a specified or understood level of assurance

[SOURCE: ISO/IEC 29115:2013, 3.15]

3.21

issuance

controlled and secure process to give the natural person identifier (NPI) holder control of their NPI ready for use

Note 1 to entry: This includes checking that the NPI holder receiving the NPI is the subject of the NPI and is able to use it for purposes conformant with the NPI policy.

3.22

legal entity

legal person or structure that is organized under the laws of any jurisdiction

[SOURCE: ISO 17442-1:2020, 3.1]

3.23

legal entity identifier

LEI

unique global identifier for legal entities participating in financial transactions and activities

Note 1 to entry: The legal entity identifier (LEI) is defined in ISO 17442-1. It is assigned by the global LEI system of local operating units with issuing registers, which are operating under the management of the Global Legal Entity Identifier Foundation (GLEIF). The GLEIF is subject to oversight by the Regulatory Oversight Committee.

3.24

legal person

individual, company or other entity which has legal rights and is subject to obligations

3.25

man-in-the-middle attack

attack in which an attacker is able to read, insert and modify messages between two parties without their knowledge

[SOURCE: ISO/IEC 29115:2013, 3.16]

3.26

morphing attack

attack in which two or more facial images are combined and presented during registration as a biometric reference

Note 1 to entry: The combined image, or morph, is designed to deceive the biometric system so that any of the persons, whose images have been combined, can successfully pass the facial biometric check.

3.27

multifactor authentication

authentication of an operator using at least two independent authentication factors

[SOURCE: ISO/IEC 19790:2025, 3.86, modified – Notes 1, 2 and 3 to entry were removed.]

3.28

mutual authentication

authentication of identities of entities which provides both entities with assurance of each other's identity

[SOURCE: ISO/IEC 29115:2013, 3.18]

3.29

natural person

human being with fundamental human rights

3.30

natural person identifier

NPI

global identifier for natural persons involved in financial transactions

3.31

non-repudiation

ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action

[SOURCE: ITU-T X.1252: 04/2021, 6.61]

3.32

NPI authorised entity

legal entity authorised to access specific personal information in a natural person identifier (NPI) register

Note 1 to entry: The authorised legal person in the legal entity is expected to have an NPI.

3.33

NPI community

community of natural person identifier (NPI) issuers, holders, registers, authorised entities and governance organizations as well as authoritative NPI data sources

3.34

NPI community architecture

structure and processes within the natural person identifier (NPI) community for the conformant use of an NPI and support for the NPI lifecycle

3.35

NPI data

data and metadata related to the compliant use of a natural person identifier (NPI) and support for the NPI lifecycle

3.36

NPI federation

federation of natural person identifier (NPI) registers and NPI authorised entities

3.37

NPI governance body

global body responsible for all aspects of governance and risk management relating to the natural person identifier (NPI)

Note 1 to entry: This includes requirements, policies, procedures, mechanisms, data, operations, finance, commercial, legal, and regulatory compliance, risk mitigation strategy, fraud and anomaly detection, incident management, investigations, support for prosecution and court processes, and remedies for victims.

3.38

NPI holder

natural person who is the subject of the natural person identifier (NPI) data and controls consent for third party access to the data

Note 1 to entry: Authorities can have access to this NPI data without consent if authorised by statute law or a court of law.

3.39

NPI issuer

certified neutral organization responsible for the enrolment, registration, issuance and management of a natural person identifier (NPI) throughout the NPI lifecycle, and the management of an NPI register

3.40

NPI lifecycle

phases during the lifespan of a natural person identifier

3.41

NPI record

set of attributes in a natural person identifier (NPI) register that are linked or bound to the NPI

3.42

NPI register

repository of natural person identifiers (NPI) managed by an NPI issuer

Note 1 to entry: The NPI register contains NPI data for active, suspended and revoked NPIs, and a record of all NPIs recorded and issued by the register.

3.43

NPI register architecture

structure and processes operating with and across all natural person identifier (NPI) registers for the conformant use and operation of the NPI and support for the NPI lifecycle

3.44

NPI system

technical system that is connected to one or more natural person identifier (NPI) registers for the purpose of supporting the safe and conformant operation of the NPI lifecycle

3.45

NPI trust framework

policy framework governing the natural person identifier lifecycle by all actors

3.46

NPI recordset

a data structure that consists of a group of natural person identifier database records that is from a base table or as the result of a query

3.47

phishing

scam by which an email user is duped into revealing personal or confidential information which the scammer can then use illicitly

[SOURCE: ISO/IEC 29115:2013]

3.48

privacy

legal right to the protection of personal or private information from misuse or unauthorised disclosure

3.49

processing of personal data

operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

[SOURCE: ISO 25237:2017, 3.40]

3.50

registration authority

trusted actor that establishes and/or vouches for the identity of an entity to a credential service provider

[SOURCE: ISO/IEC 29115:2013, 3.21]

3.51

provisioning

process of issuing trusted digital artefacts including credentials, permissions, cryptographic keys and authorisations to an authenticated entity according to policy

Note 1 to entry: Similarly, deprovisioning is the removal of the same.

3.52

relying party

actor that relies on an identity assertion or claim

[SOURCE: ISO/IEC 29115:2013, 3.22]

3.53

repudiation

denial in having participated in all or part of an action by one of the entities involved

[SOURCE: ITU-T X.1252: 04/2021, 6.77]

3.54

revocation

permanent withdrawal or cancellation of an agreement or legal artefact

3.55

salt

non-secret, often random, value that is used in a hashing process

Note 1 to entry: It is also referred to as sand.

[SOURCE: ISO/IEC 29115:2013, 3.24]

3.56

shared secret

secret used in authentication that is known only to the entity and the verifier

[SOURCE: ISO/IEC 29115:2013, 3.25]

3.57

time stamp

reliable time variant parameter which denotes a point in time with respect to a common reference

[SOURCE: ISO/IEC 29115:2013, 3.26]

3.58

transaction

discrete event between two entities that supports a business or programmatic purpose

[SOURCE: ISO/IEC 29115:2013, 3.27, modified — The term "between an entity and service provider" was replaced with "between two entities".]

3.59

trust framework

set of requirements and enforcement mechanisms for parties exchanging identity information

[SOURCE: ISO/IEC 29115:2013, 3.28]

3.60

trusted third party

authority or its agent, trusted by other actors with respect to specified activities (e.g. security-related activities)

Note 1 to entry: A trusted third party is trusted by an entity and/or a verifier for the purposes of authentication.

[SOURCE: ISO/IEC 29115:2013, 3.29]

3.61

validation

digital and cryptographic check of a claimed attribute against the authoritative source

3.62**validity period**

time period during which an identity or credential is used in one or more transactions

[SOURCE: ISO/IEC 29115:2013, 3.30]

3.63**verification**

process of checking information by comparing the provided information with previously corroborated information

Note 1 to entry: This can include documents or data.

[SOURCE: ISO/IEC 29115:2013, 3.31, modified — Note 1 to entry was added.]

3.64**verifier**

actor that corroborates identity information

Note 1 to entry: The verifier can participate in multiple phases of the enterprise authentication assurance framework and can perform credential verification and/or identity information verification.

[SOURCE: ISO/IEC 29115:2013, 3.32]

3.65**virtual NPI**

short lifetime natural person identifier (NPI), bound to the NPI already issued

Note 1 to entry: This is a counter-fraud measure to protect the NPI. Its lifetime is measured in days.

4 Abbreviated terms

The following abbreviated terms are used in this document. They are common across standards associated with information risk management, identity management and privacy protection.

AML	anti-money laundering
BMS	biometric matching service
CBDC	central bank digital currency
CCSA	collaborative cyber situational awareness
CERT	computer emergency response team
CDD	customer due diligence
CFT	countering the financing of terrorism
CIR	common identity repository
CNI	critical national infrastructure
DLT	distributed ledger technology
DNS	domain name system
EDD	enhanced due diligence
EoI	evidence of identity

eMRTD	electronic machine-readable travel document
EAAF	entity assurance authentication framework
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
FATF	Financial Action Task Force
FIDO	fast identity online
FISMA	Federal Information Security Modernization Act
GNPIA	global natural person identifier authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICAO	International Civil Aviation Organization
ID4D	identity for development
IdSP	identity service provider
KYC	know your customer
LEA	law enforcement agency
LEI	legal entity identifier
LoA	level of assurance
LoIP	level of identity proofing
MID	multiple identity detector
MLC	message less compute
NPI	natural person identifier
OECD	Organization for Economic Co-operation and Development
P2P	peer to peer
PAD	presentation attack detection
PCTF	pan-Canadian trust framework
PEP	politically exposed person
PET	privacy enhancing technology
PII	personally identifiable information
PIN	personal identification number
PMO	program management office
RUA	returning user authentication
SANS	sysadmin, audit, network and security

SMPC	secure multi-party computation
TDA	technical design authority
vLEI	verifiable legal entity identifier
ZKP	zero knowledge proof

5 NPI standard: ISO 24366

ISO 24366 describes the format and data record for the NPI.

It states that the NPI meets the needs of the global financial services industry and the regulatory community for natural person identification. Key provisions include:

- enabling unique identification globally of natural persons requiring an identifier (see ISO 24366:2021, Clause 4);
- defining an NPI code that contains no embedded intelligence (see ISO 24366:2021, Clause 4);
- ensuring the NPI code is interoperable with other standards and existing reference data, and can be applied globally to support the financial services industry (see ISO 24366:2021, Introduction);
- leveraging the expertise of ISO/TC 68, *Financial services*, in defining and maintaining identifier standards (see ISO 24366:2021, Introduction);
- defining an NPI scheme that is reliable and an NPI code that is persistent (see ISO 24366:2021, Clause 4);
- defining an NPI scheme that is extensible and free from limitations on use and redistribution (see ISO 24366:2021, Introduction).

Additionally, it notes that it is possible that already existing national NPIs are not applicable in cross-border transactions (see ISO 24366:2021, Introduction).

The NPI defined in ISO 24366 aims to close this gap, to provide an interoperability mechanism for national NPIs and the NPI, enabling their co-existence.

Since ISO 24366 was published, additional provisions and requirements have emerged, which are considered in [Clause 6](#).

6 Overview of requirements

6.1 Introduction

The number of potential use cases of the NPI to benefit a community of interest is growing every day. These arise from discussions with governments, regulators, industry sectors and individual organizations. Each of these use cases has relevant business requirements that depend on strong identification and identifiers, as well as strong data governance and risk management. Because of the significant scale of supply and financial process networks, the NPI and its operation and governance are expected to offer levels of assurance and confidence that are well above that of individual participating organizations. Therefore, the NPI initiative requires sufficient understanding of important use cases, their major business requirements and the functional requirements that can be derived from an analysis of the business requirements.

Many of the requirements are described further in [Clause 12](#) and several annexes, including the requirements and policy documents of international organizations in [Annex F](#).

6.2 Business requirements

For the mapping of the NPI against other identifiers to help shed light on the wider use case/business case links and potential benefits and more details, see [Clause I.2](#).

Over 70 use cases have been identified. Common business requirements have been identified across these use cases, resulting in a reduction of exemplar use cases to 22, without losing any of the major business requirements. See [Annex I](#).

6.3 Functional requirements

Functional requirements can be identified from business requirements and real-world risk factors. These functional requirements define a baseline above which the NPI is expected to operate. If the NPI is unable to meet this baseline of functional requirements, some countries and user communities will be unable to use the NPI. The purpose of the NPI will therefore not be achieved and the global communal benefits will be diminished. Conversely, some countries or industry sectors can struggle to satisfy the NPI's functional requirements and can require assistance. However, that assistance cannot compromise the baseline of functional requirements, particularly with regard to the policy requirements for counter-fraud, data quality management and cybersecurity risks.

Management and decision-making in almost all business (government and industry) organizations can be expressed in terms of risk, e.g. direct harm to the business, reputational damage, inability to seize business opportunities and reduction in competitive advantage. But they also include shared cyber and information risks associated with supply chains, distribution chains, partnerships and customers; shared risks require collaborative risk mitigation. An organization cannot mitigate shared risks by itself.

The analysis of these typical organizational and shared risks is reflected in the baseline of functional requirements.

7 Risk and risk mitigation considerations

7.1 General

7.1.1 Major types of risk

The NPI faces all the major risks of any digital organization, but it also faces other types of risk associated with scale and critical national infrastructure.

The major types of risk are normally considered for an organization or a group of cooperating organizations, e.g. in a supply chain. Within each type, an organization has internal risks that it can mitigate and risks that are shared with other organizations that can only be mitigated effectively by collaboration. A lack of consideration of external collaboration risks is an indicator that an organization's risk mitigation strategy is ineffective and that the organization is vulnerable.

7.1.2 Compliance risk

All legal organizations are expected to comply with laws and regulations, most of which concern the safe and secure operation of the organization, including all its policies, procedures and technical mechanisms. The risk mitigation strategy normally includes requirements for external, independent assessments and certifications. This significantly affects the NPI design, implementation and operations.

New legislation for know your customer (KYC), anti-money laundering (AML), privacy and other requirements for information protection and identification continue to emerge. All financial services have legal requirements for basic customer due diligence (CDD) and, in some cases, enhanced due diligence (EDD) to address new risks and threats. There is some variation of national CDD and EDD legislation, primarily because some jurisdictions are further ahead in strengthening their CDD and EDD as they expand their digital economies and societies. Further information can be found in [Annex B](#).

An example is the Portuguese government legislative requirements for enrolment and identity proofing in compliance with international standards, which supports their Chave Móvel Digital (CMD), or Digital Mobile Key, used for authentication in government and consumer services, and which is European Union (EU) eIDAS compliant. [Reference \[6\]](#) is an extract from the regulation.

Governments, including those in the EU, seek stronger risk and mitigation techniques for countering financial crime and wider fraud, such as tax evasion, VAT fraud, benefits fraud, Covid payment fraud and more. A growing number are referencing international standards in their legislation and establishing schemes for certification and accreditation. The NPI is therefore expected to take account of many of these standards if governments are going to accept that the NPI is regulatory compliant.

7.1.3 Complexity risk

Most organizations depend increasingly on complex digital systems to support all their business operations, to the extent that they cannot compete or operate effectively without them and the increasingly complex data that they contain. The quality of decision making within an organization directly depends on the ready availability of high-quality corporate data, which includes personal and other data related to the NPI itself and its use. The NPI addresses relevant complexity risks. For example, a major complexity risk is ensuring that a person cannot obtain or use two or more NPIs globally, which requires the detection of duplicate natural persons and identities across all the NPI registers operating worldwide.

Further information on data quality management can be found in [Annex E](#).

7.1.4 IT/cybersecurity risk

Digital systems (communications, networks, cloud services, applications, devices, computers, phones, sensors, cameras, monitors, etc.) face an array of risks, which can combine to create an attack surface. The risks in the attack surface include vulnerabilities, which are weaknesses in the design or implementation of a device or system, and threats, which usually involve deliberate attacks by some form of hostile or criminal organization usually designed to disable a system or steal its data for financial advantage. Historically, the biggest risk is insider threat, which is a person within an organization who either deliberately, unknowingly or accidentally provides an attacker with the means to disable the system or access it illegally.

Weak access control systems are a common cause of successful cyber-attacks. The NPI governance and operations are expected to have strong and sophisticated access control mechanisms to meet a range of policy requirements, particularly for privacy and the protection of personal data (these are not the same).

It is possible that some or many nations require the NPI's policies, procedures and mechanisms to satisfy standards of assurance associated with critical national infrastructures. Cybersecurity is considered further in [Annex C](#).

7.1.5 Fraud risk

There are many types of fraud related risk and the number is growing. Impersonation and identity theft are significant. The NPI risk mitigation strategy monitors and mitigates relevant fraud risks if the NPI is to be trusted.

7.1.6 Identity management risks

The creation, issuance, use and management of NPI-related identity and identification information presents identity management risks that the NPI addresses.

7.1.7 Data quality risk

The accuracy and quality of personal data at a given point in time is critical to defeating a range of threats to and vulnerabilities of the NPI and to related financial services. This data can be distributed and a key attribute can move between different organizations at any moment. Each NPI issuer's system is expected to manage this risk.

7.1.8 Opportunity risk

Opportunity risks involve the inability of an organization to seize a commercial or government opportunity because it cannot mobilise its resources or make decisions fast enough. It misses commercial opportunities and is less competitive. The NPI can reduce opportunity risk by helping to maximise data quality and

cross-organizational interoperability. It also enables re-use, which is where digital capabilities created to meet a particular set of requirements can be re-used for a completely new set of requirements without modification. Re-use reduces business friction and increases business effectiveness and competitiveness, and the equivalent in government organizations. Re-use is a top business requirement in many industry sectors, but this appreciation is not yet so apparent in the financial sector. The NPI helps the financial sector reduce its opportunity risks in many areas.

Opportunity risk is beyond the scope of this document.

7.1.9 Branding/reputation risk

Major government and industry organizations go to great lengths to protect their branding and reputation, which, if damaged, can reduce their competitiveness and effectiveness, and also incur significant cost and resources to repair. For companies, it can dramatically reduce their share price and can even force them out of business. Mitigation measures are many and varied and require highly accurate situational awareness throughout the organization, particularly at board level. The NPI can contribute to this.

Branding and reputation risk is beyond the scope of this document.

7.2 Scope of use and liability

The liability of organizations, particularly service providers, depends on the scope of use, which is reflected in the contractual terms and conditions agreed by the customer. The United Nations Commission on International Trade Law (UNCITRAL) is working on the limits of liability for identity service providers (IdSPs). For the NPI, the main concern is where a customer uses their NPI identity information or NPI credential in a way that is outside the contracted policies or terms and conditions, and this adversely impacts third parties who seek legal remedy or compensation from the IdSP. The NPI is expected to require a policy and governance mechanisms to support limits of liability for its service providers, particularly NPI issuers.

The Commonwealth Law of Virginia has terms on liability and limits of liability that are often referenced in other jurisdictions. § 59,1-552 of the code of Virginia includes a limitation of liability: “An identity trust framework operator or identity provider shall not be liable for misuse of an identity credential by the identity credential holder or by any other person who misuses an identity credential”. [\[18\]](#)

Other jurisdictions are working on models for liability and limits of liability. Further details are beyond the scope of this document.

7.3 Risk mitigation policies

As work to develop, implement, operate and use NPIs expands, it will be important to distinguish between risks specifically to the NPI itself versus risks to all NPI users.

7.4 Risk mitigation strategy

7.4.1 General

Many risk management frameworks exist but only a few cover the overall spectrum of digital risk and across a community of organizations, such as a supply chain or an industry, upon which a risk mitigation strategy can be developed. National examples include the following:

- Estonian information security standard; [\[19\]](#)
- German BSI 200 series; [\[20\]](#), [\[21\]](#), [\[22\]](#), [\[23\]](#)
- US NIST Cybersecurity Framework; [\[24\]](#)
- Chinese TC260 standards. [\[25\]](#), [\[26\]](#)

Commercial examples include COBIT and SANS/Center for Internet Security. [\[27\]](#), [\[28\]](#) See also ISO 31000, ISO/IEC 27001 and ISO/IEC 27002.

Almost all citizens are entitled to make decisions to protect their personal data and themselves. They increasingly rely on some form of assistance or automation to do so. All these decisions involve risk for which some form of risk mitigation is expected. As with any data-driven digital situation, the NPI requires a risk mitigation strategy. This is at the core of a collaborative governance strategy underpinning the exploitation of NPI to deliver tangible benefits.

The NPI can use [Figure 1](#) based on standards such as ISO 31000, ISO/IEC 27000 and US SP800-53^[30] as a foundational input upon which to develop a risk mitigation strategy that informs technology implementation, testing, assurance and operations. The five main steps typically include:

- identify (the risk);
- protect;
- detect;
- respond;
- recover.

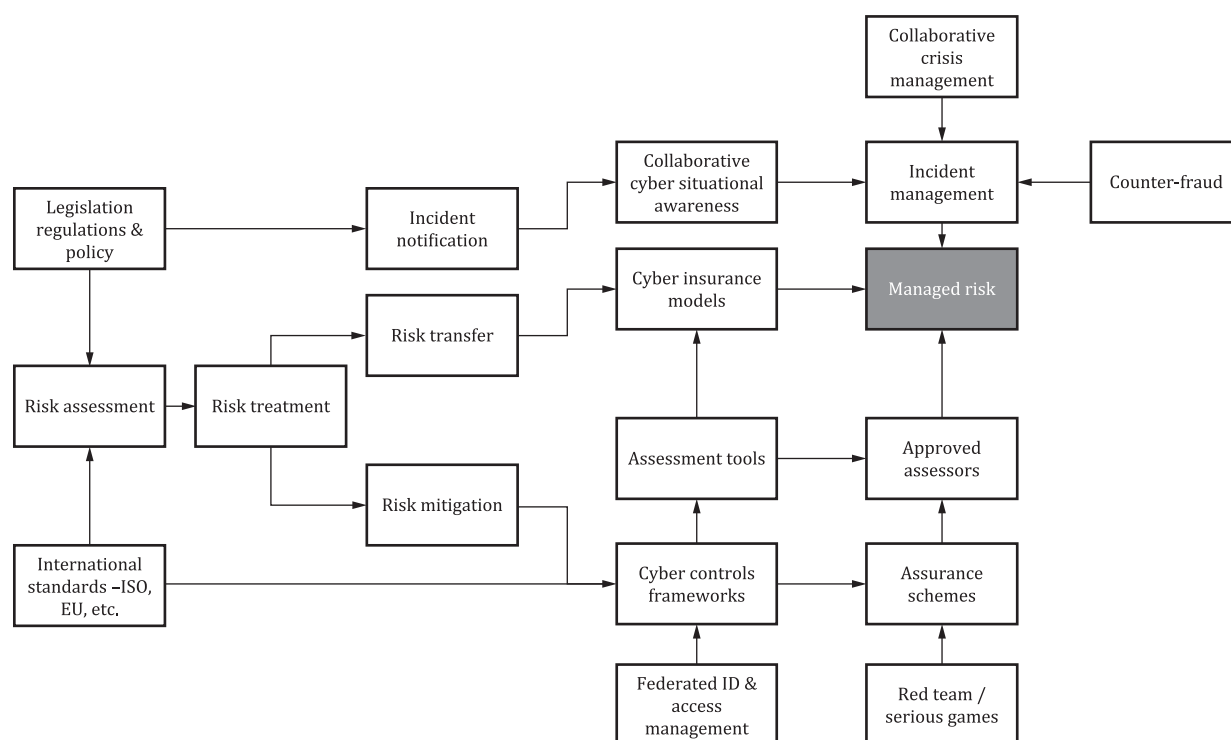


Figure 1 — NPI risk mitigation context

7.4.2 Identify

Identifying the risk and assessing it (compliance, complexity, cyber etc). The failure to identify risks is the single biggest contributor to cyber and counter fraud incidents. The NPI governance and operations will identify and catalogue the risks associated with each business use case scenario, taking into account legislation, regulations and policy, as well as international standards and best practices. These risks will include a wide range of threats and vulnerabilities including cyber (hardware and software), identity, privacy, data quality, insider threats, human failures, misbehaviours and anomalies. They will also include regulatory compliance risks such as the EU General Data Protection Regulation (GDPR), the EU Cybersecurity Act and many international financial regulations, including reporting regulations.

7.4.3 Protect

Protecting against threats and vulnerabilities associated with the risk maintains the security and integrity of all systems and data. No protection is perfect; it cannot prevent all eventualities. The purpose of protection is to buy time to detect and respond to threats and attacks. The first step is to assess the risks that have been identified in terms of likelihood and impact, particularly taking into account the human, data, software and hardware perspectives, and then to treat each risk to decide whether to:

- Transfer the risk, normally using cyber insurance. However, this only applies to financial risks. It is not appropriate in most cases of non-financial regulatory compliance risk.
- Mitigate the risk using a range of appropriate cyber and other controls within the risk mitigation strategy, based on strong, federated identity and access management. It is possible that this requires leveraging privacy enhancing technologies (PETs) such as zero knowledge proofs (ZKP), secure multi-party computation (SMPC), message less computation (MLC) and homomorphic encryption to avoid almost all possibility of exposure of personal data outside of the organization, application or device. It can also include the use of very high assurance hardware containers for key management, potentially including dual roots of trust.
- Accept the (residual) risks. All major risks are normally mitigated in some way, but it is possible that there are remaining, residual risks that have to be accepted. They cannot be ignored without creating further risks to organizations.

7.4.4 Detect

Detecting that the risk is now happening and is a threat or an incident. This assumes:

- a) that there is an agreed, detailed baseline for normal operation;
- b) the means exist to detect anomalies or abnormalities that require a response.

Detection is a vital part of any mitigation strategy.

The NPI uses a mix of deterministic and stochastic approaches to detect anomalies and pre-defined indicators of compromise. Advances in artificial intelligence (AI) and machine learning technologies have the potential to help significantly. The results are fed into and inform a collaborative cyber situational awareness (CCSA) capability that provides a single view of what is going on. The results then feed into the incident management process, which the NPI's operational governance is expected to have.

Any system is expected to have a notion of normality if it is to detect abnormalities. This typically involves the use of a corporate security information and event management capability for network management as a basic capability. The NPI governance develops a basic cyber situational awareness capability that can be used to inform the incident management process and act as a bridge for computer emergency response teams (CERTs), information sharing and analysis centres and similar collaborative organizations, as well as law enforcement agencies (LEAs).

A similar organizational approach and capability is taken for counter-fraud.

7.4.5 Respond

Responding to the incident is crucial. The response normally has two purposes: to contain and neutralise the threat or attack; and to ensure the continuity of business or functional operation. Ideally, the user is largely unaware of the response in most cases, but more significant attacks, for example ransomware, require not only the user to be involved but also other parties, including CERTs and LEAs. Effective NPI governance relies on the ability to address risks and to respond to events and incidents. In particular, it focuses on those affecting or misusing personal data.

7.4.6 Recover

The final stage is to recover to normality. The NPI governance brings all these aspects together as part of the risk mitigation strategy that informs the technology implementation, testing and selection of suitable assurance schemes. As part of this, the NPI governance:

- ensures the strategy reflects the requirements and risks arising out of the use case scenarios as well as generic cyber, human, etc. risks to personal data and users;
- considers how best to manage change and dynamic risks, building on cyber situational awareness;
- seeks to leverage the latest technologies and techniques, including from CERTs and LEAs to mitigate risks;
- feeds into, and feeds back from, the technology implementations, testing, assurance and monitoring.

8 Policy considerations

8.1 Major policy considerations

8.1.1 General

Major policy considerations concern factors around uniqueness, scale, performance, extensibility, interoperability and the realisation of potential benefits.

The possibility of there being a single, central register for all NPIs is not considered feasible for three reasons:

- Political: It is possible that countries do not agree to it in principle, and that they do not accept their country's NPI citizen data being held in another country in significant volume.
- Legal: Variations in national legislation, particularly regarding privacy and the protection of personal data, preclude this.
- Security: Centralising such data entails creating a massive single point of failure, with no meaningful resilience, as well as providing an invitation to criminal organizations and hostile countries to attack it or at least prevent its use by others.

Many other digital networks, including the internet and mobile phone networks, operate distributed registers for reasons of resilience, security, performance and scale. The NPI is expected to do the same. It is expected to operate NPI registers around the world in most, if not all, jurisdictions. These can be operated by government or industry organizations or both within a global federation model.

8.1.2 Uniqueness

The NPI is currently required by policy, based on legal norms and best practices, to be globally unique and to link to only one person. The following are therefore true:

- Each NPI, as a number, is globally unique and therefore exists authoritatively in only one NPI register.
- Each NPI can only link to one person. It cannot be shared, transferred or re-used.
- A natural person can only exist once within one NPI register with one NPI. For the same person to have more than one NPI in a register would break the normal integrity rules for any identification system and create significant opportunities for fraud that would be almost impossible to prevent.
- A natural person can only have one NPI globally. By extension and for the same reasons, the same policy applies across all NPI registers globally.
- The NPI would normally be issued within the country that they reside, not the country for which they hold a passport or a different country where they work.

- Relying party organizations seeking to validate the NPI for a person can validate the NPI for that person, but, if authenticated and authorised, the relying party can also request specific personal data attributes linked to the NPI. The relying party will require uniqueness and will depend upon it in their business processes.

However, abnormal circumstances are possible where a person has two or more NPIs globally. This situation would be considered non-compliant and require a means for detection and immediate rectification to restore compliance.

Alternative options have been considered and discarded as legally non-compliant, too difficult, too risky or too complex. The following options were considered and discarded completely as being unacceptably risky:

- a) Changing a person's NPI if they change a country of residence. There is only one NPI for each person during their lifetime, wherever they reside.
- b) Allowing a person to change NPIs but having only one NPI for a person at any moment in time. This assumes that:
 - 1) They relinquish their NPI from one NPI register before they can receive a new NPI from a different register.
 - 2) The two (or more) NPIs are linked globally to ensure traceability and data coherence. This was considered too difficult to manage globally.
- c) Allowing a person to have two or more NPIs at any given time, each from a different register. This was considered an unacceptable fraud risk that can destroy trust in the NPI.

8.1.3 Scale

As a global identifier that is frequently used, the size of the NPI would have to be larger than any other natural person or citizen identifiers. Based on the experiences of large national digital identification systems, here are the sizing estimates for the NPI as a whole and for an individual NPI register:

- The NPI Trust Framework has 4 billion active users at any time and 500 NPI registers.
- The planning lifetime for a typical NPIs is 80 years, however an individual NPI can last for longer.
- The planning duration of the NPI Trust Framework is 100 years after which it will be replaced.
- Assuming 50 years average longevity of an NPI holder and a maximum world population of 10 billion people gives an overall maximum lifetime population of 30 billion NPIs.
- Allowing for errors, fraud and natural disasters, the overall volume is sized at 100 billion NPIs.

These numbers can be increased but it is unlikely that they will be reduced.

The capacity of the NPI as a calculated identification code allows additional entropy to cope with random collisions in the calculations. For example, if this entropy is a factor of 10, then the capacity of the code format is at least 1 trillion NPIs (1 000 000 000 000).

Sizing for one NPI register involves several considerations. Each register can have different numbers and types of biometrics. The biometric entropy is specific to the country's population size.

8.1.4 Performance

When an NPI or virtual NPI is being used to support a transaction, the validation of the NPI or the detection of an anomaly is expected to respond within a few seconds, even during peak periods.

Access to specific personal data by NPI authorised entities is expected to be similarly responsive.

8.1.5 Extensibility

The current set of data attributes in ISO 24366 can be expanded in the future with additional data attributes. All NPI registers and deduplication systems are expected to be extensible to incorporate these additions.

8.1.6 Interoperability

All NPI registers are expected to be interoperable and conform to ISO 24366. If two or more NPI registers have additional attributes that are not listed in ISO 24366, but which are semantically similar, every effort would be made by the global NPI authority (GNPIA) to align these both semantically and syntactically and bring them into the NPI data model.

8.1.7 Realisation of potential benefits

Successful governance of the NPI depends on the confidence of its users whenever they use the NPI. Capturing, measuring and communicating tangible benefits realised by using the NPI frequently on a large scale will boost the overall level of confidence.

8.2 Outline process: NPI lifecycle

A high-level view of the NPI lifecycle is shown at [Figure 2](#). This is based on accepted norms, regulations and international standards. It shows the happy path when an application is successful and the NPI holder can use their NPI normally. The management layer normally contains operational governance functions including three major processes:

- a) the unhappy path, which is the processes that deals with problems associated with the subject during enrolment and the NPI holder after the NPI is issued;
- b) maintenance activities during the use phase, which ensure data quality, service availability and customer service;
- c) monitoring to ensure collaborative situational awareness across all NPI issuers, risk minimisation, systems integrity and conformant use of the NPI. This also includes collaborative threat and anomaly detection, and collaborative incident response, as well as counter-fraud and cybersecurity incident investigations.

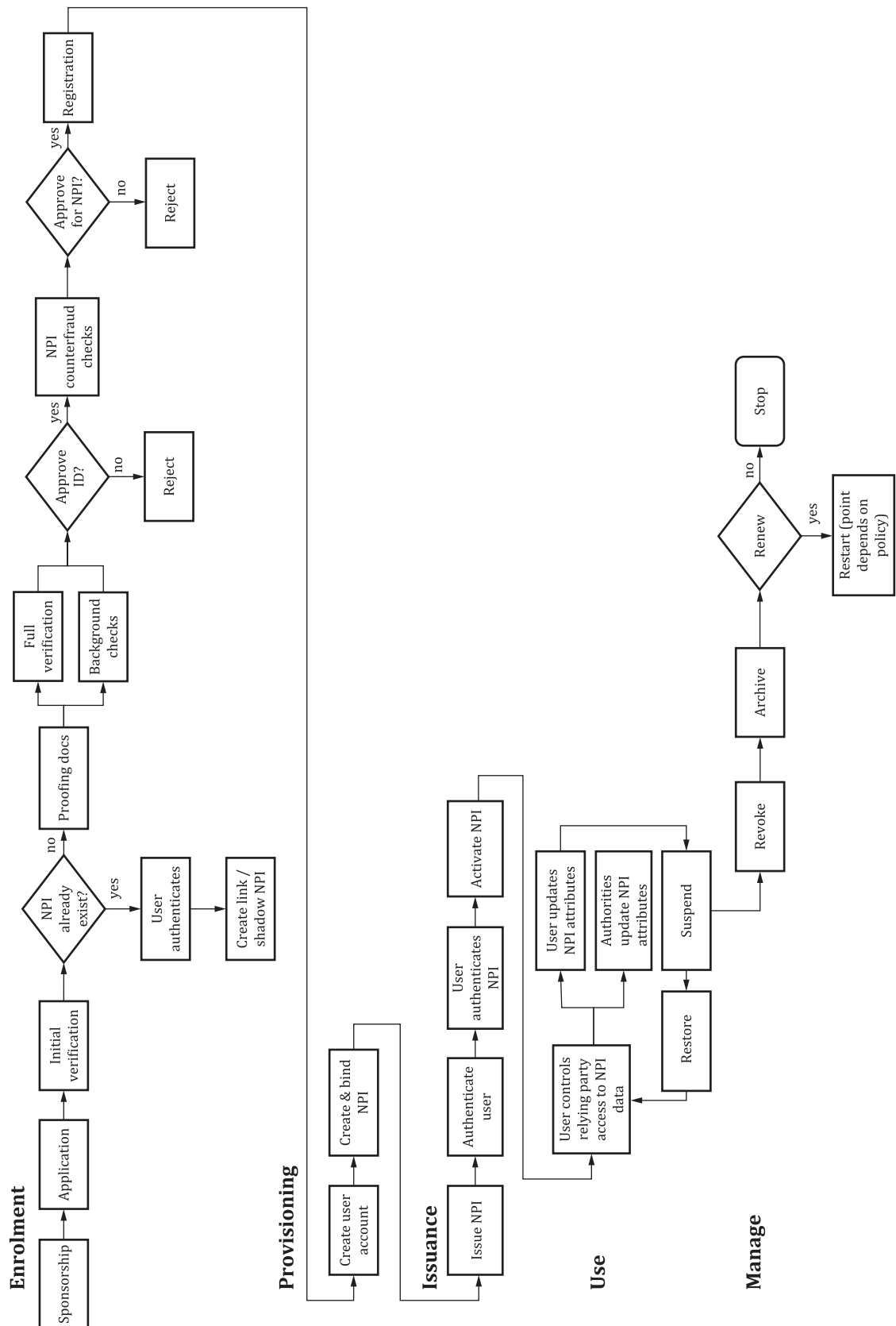


Figure 2 — NPI lifecycle

8.3 User journey

A typical user journey is as follows:

- The user applies to open a bank account.
- The bank asks the user for their NPI, but the user does not have one.
- The bank redirects the user to an appropriate NPI issuer in the jurisdiction in which the user resides or in the jurisdiction that issued the user their government-issued identity documents.
- The user applies to the NPI issuer, successfully completes enrolment and is registered in the NPI register. The user is now an NPI holder.
- The user returns to the bank and presents their NPI to the bank to complete the process to open a bank account.

It is possible that there is a need for flexible interpretation regarding where the user resides. Typically, this is the jurisdiction in which the user pays taxes, has a tax identification number and uses physical government services regularly – education, health, waste etc. Where this is not possible or applicable (e.g. for military, diplomatic or UN staff overseas), the NPI issuer is normally where they are domiciled. That is usually their country of origin, where they are a citizen and are entitled to a passport.

8.4 Main actors in the NPI lifecycle

8.4.1 General

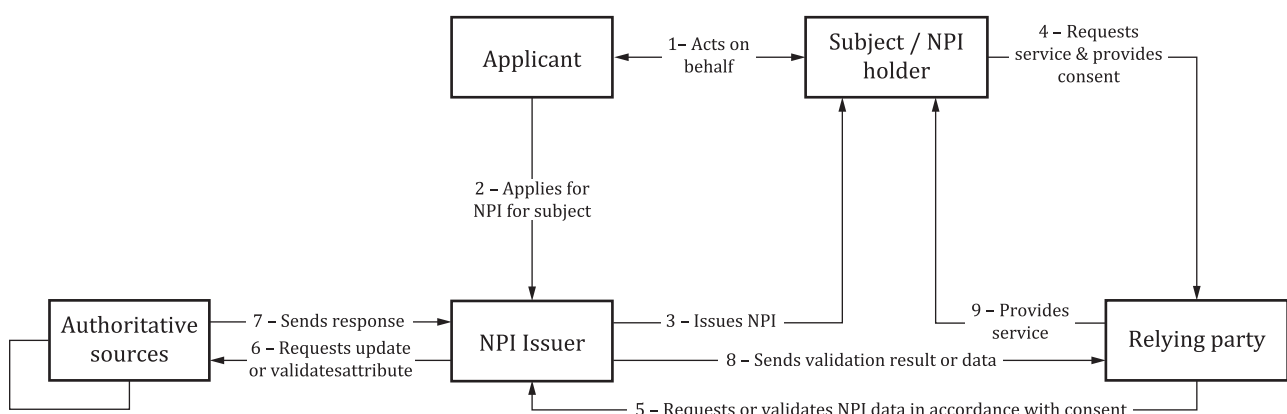


Figure 3 — NPI actor diagram

[Figure 3](#) shows high level processes for obtaining and using an NPI with the main actors in this process. These processes are part of the overall lifecycle of an NPI, from its creation to its permanent end.

The main actors in the envisioned NPI lifecycle are:

- The subject who becomes the NPI holder.
- The NPI holder, who possesses their NPI and controls relying party access to the associated personal attributes, granting consent, as necessary. They seek a service from the relying party, which can require them to provide their NPI and/or some attributes linked to the NPI.
- The NPI issuer, which operates the NPI lifecycle and an NPI register. It assures the quality and accuracy of the data provided to the relying party. It manages the NPI data contained in the register. It works with other NPI registers and organizations as necessary for the purposes of ensuring data quality and policy compliance, and for detecting fraud and other anomalies for immediate response and further investigation. The NPI issuer operates as a trusted third party.

- The authoritative sources for each attribute bound to the NPI as listed in ISO 24366. Each source acts as a trusted third party.
- The relying party, who requires an existing or potential customer to provide their NPI and a limited set of permitted attributes necessary for the business purpose, with the customer's consent. For example, for a new customer opening an account, the relying party can choose to validate a customer's NP, and personal data claimed by the customer against the NPI register.
- The GNPIA, which provides the governance across the creation, issuance, use and lifecycle management of all NPIs and operates the federation of NPI issuers to ensure that their NPI register operations can be trusted by all parties. The GNPIA:
 - does not hold copies of NPI personal data held by individual NPI registers: there is no central database or data centralisation;
 - provides deduplication between and across NPI registers to prevent a person holding more than one NPI or to detect anomalies indicating persons attempting to commit fraud. This is done using mathematically based PETs, possibly including hash functions, ZKP, SMPC, MLC and homomorphic encryption;
 - provides services to enable very high data quality within and across all NPI registers;
 - provides services to ensure that operational security, privacy and regulatory compliance is maintained across all services providing and using NPI services.

A relying party can also be a service provider to a second relying party in a chain of trust. The second relying party sees the first relying party as a trusted intermediary. This can be repeated to form a longer chain of trust. In practice, such chains are relatively short to minimise costs, risks and delays.

Where the relying party requires access to NPI holder personal data attributes, they will need to be enrolled as NPI authorised entities.

Other trusted third parties can exist. Examples include:

- Identity providers: Trusted providers of identity attributes that can also be checked in the identity proofing process to detect identity fraud indicators and data anomalies.
- Trust service providers: Trusted providers of non-identity attributes and cryptographic principals.

8.4.2 Actor enrolment

8.4.2.1 General

Each actor is known to the NPI system in sufficient detail, to manage relevant risks.

8.4.2.2 NPI issuer

A government or industry legal entity can apply to become an NPI issuer and operate an NPI register, for which there would need to be an NPI issuer enrolment process overseen and operated by a GNPIA.

Before they can be allowed to operate, candidate NPI issuers are expected to show that they have followed normative international standards and follow the guidance therein for NPI issuer operations. This is independently assured and certified by GNPIA approved assessors.

The GNPIA operates the global register of the NPI issuers and their registers, ensures their conformant operation and oversees the management of the lifecycle of each NPI issuer. It also manages the detection,

investigation and remedy of any differences, anomalies or conflicts involving NPI data within and between NPI registers.

- NPI registers are independent of each other. Each NPI is unique to an NPI register. There is no duplication of NPIs or of NPI data across registers. Policies, procedures and mechanisms to ensure that this happens are described in register operations.
- There is no information exchange between NPI registers. If a request is made to a register for NPI data held in a different register, the request is redirected to the correct NPI register.
- Access by financial institutions, especially for transnational institutions that serve the same natural person in different jurisdictions, would have to be to the appropriate NPI register. Relying party requests, such as those from financial institutions, across national boundaries would be subject to common policy in the NPI Trust Framework. It is expected that the same policies apply in all jurisdictions. However, it is possible that some jurisdictions have additional, legal requirements for their NPI registers. How these different legal requirements are met is a matter for the overall NPI governance body and the GNPIA operating body to determine.
- It cannot be possible for a specific attribute to have a different meaning in different NPI registers. Semantically, each specific attribute would need to be the same in every NPI register, even though their syntax can differ.
- The approach of both financial institutions and applicants to access the register of a specific NPI would need to be described in the IT deployed logical structure.
- The minimum normative controls in the access control model would need to be described in an NPI-related international standard.
- The policies and procedures of an NPI issuer are similar to those of a credential service provider and the NPI issuer's operation of its NPI register makes it also a registration authority.

8.4.2.3 NPI authorised entities

All interactions with data held on an NPI register are expected to conform to the NPI access control policy, whereby the party accessing the register is known to the register and is able to comply with the access control policy.

It is possible that any relying party or authority requiring validating only personal data attributes for an NPI to prove possession by the NPI holder of the NPI can do so with user consent or with proper legal authority authorised by legislation or a court of law.

However, any relying party or authority requiring validating or have access to personal data in an NPI register associated with an NPI, and who have legitimate interest to do so, would need to be known and authorised. A relying party first enrolls as an NPI authorised entity with the NPI issuer and register for authentication credentials and access permissions that meet the legitimate interest and purpose. These credentials and permissions are specific to each NPI register (i.e. there is no need for federated identity and access management across NPI registers, although this can change).

Where there is a legal requirement for user consent, the NPI issuer manages user consent according to recognised standards such as ISO/IEC TS 27560.

9 Framework considerations: Entity Authentication Assurance Framework

9.1 General

This clause provides examples of frameworks for the use of NPI. NPI operations focus on the creation, use and management of each NPI, which has a lifecycle. A suitable framework for managing the NPI lifecycle often

includes or is based on the Entity Authentication Assurance Framework (EAAF) described in ISO/IEC 29115. The EAAF (shown in [Figure 4](#)) consists of four main phases:

- a) identification (identity proofing) of natural persons and verification of their identity documentation and data;
- b) NPI issuance;
- c) NPI use;
- d) management of the lifecycle of the NPI.

Phases 1 to 3 are supported by the management layer (Phase 4) that describes the operational policies, procedures and mechanisms to enable the other three phases to operate effectively and safely, in compliance with the common policy or overall NPI Trust Framework issued by the GNPIA. The NPI Trust Framework is the set of policies and procedures required for the overall safe governance, operation and use of the NPI.

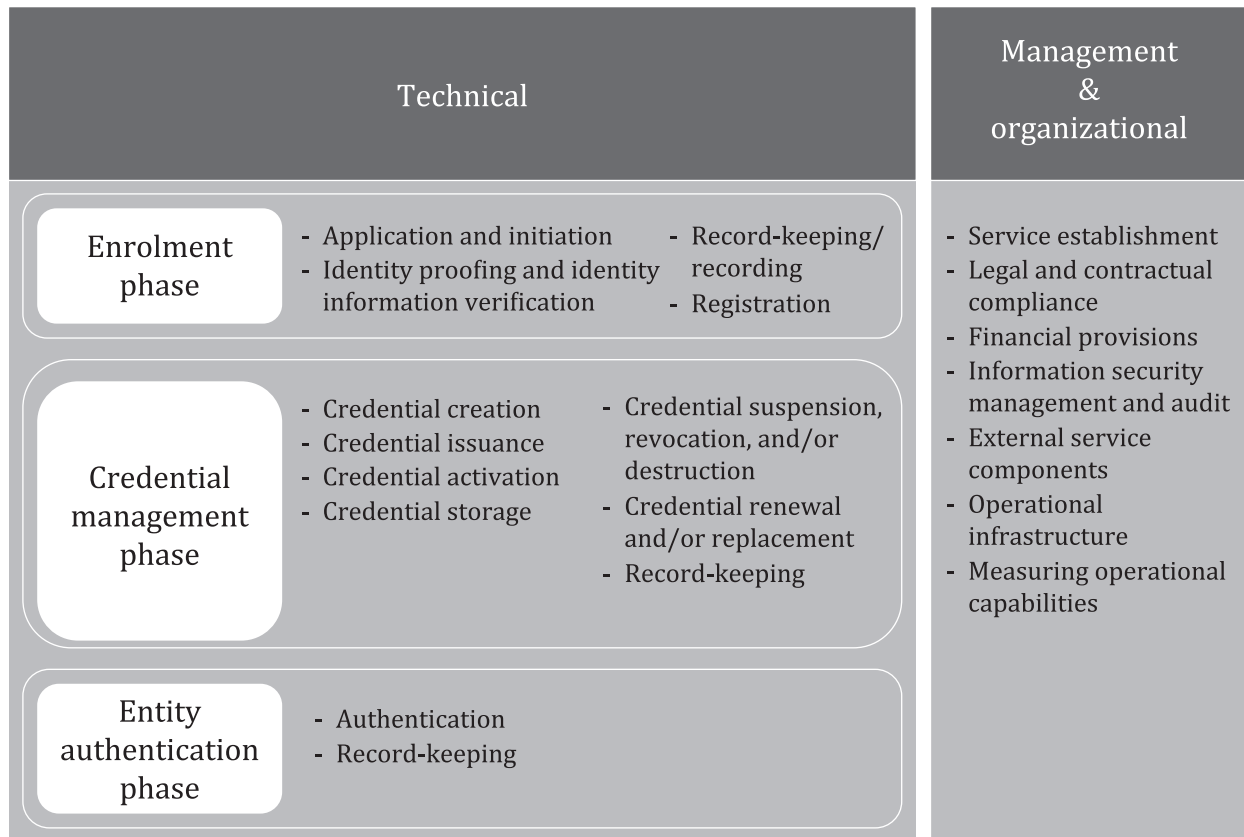


Figure 4 — Overview of the Entity Authentication Assurance Framework (ISO/IEC 29115)

9.2 Phase 1: Enrolment

9.2.1 General

The enrolment phase is a critical component of the EAAF. It establishes the foundation for secure and reliable identity verification. This phase encompasses several key steps, including the application process, identity proofing and the collection of evidence of identity. Each step is designed to ensure the authenticity and integrity of the individual's identity. The process flow outlines the sequence of actions required to achieve successful enrolment, while identity-person binding and the use of biometrics further enhance the security and accuracy of the authentication process.