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

Reference number
ISO/TR 24371:2025(en)

© ISO 2025



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

© ISO 2025 – All rights reserved

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 2025 – All rights reserved

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**

© ISO 2025 – All rights reserved

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.

© ISO 2025 – All rights reserved

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;

© ISO 2025 – All rights reserved

— 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 J. 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

© ISO 2025 – All rights reserved

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

© ISO 2025 – All rights reserved

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]

© ISO 2025 – All rights reserved