TECHNICAL SPECIFICATION

ISO/TS 42502

Sharing economy — Guidance for provider verification on digital platforms

Économie du partage — Lignes directrices pour la vérification du fournisseur sur les plateformes numériques

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Contents

Page

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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 324, *Sharing economy*.

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 sharing economy represents a new way of engaging in interactions about products and assets creating a new economic model. Although there are thousands of sharing economy digital platforms operating in almost every industry, and the global sharing economy industry generates hundreds of millions of transactions every day, many people still feel unsafe using online sharing services.

The last decade has witnessed a significant number of incidents in which many sharing platform operators failed to keep their promises of meticulous and authentic identity verification of platform providers and users, causing a negative social impact. The urgent problem facing the development of sharing economy is whether users can trust providers to provide safe and effective products and assets.

It's crucial to clarify the responsibilities of providers and platform operators and strengthen the platform operators' verification of identity and credentials of providers, which will better maintain the stable, healthy, and sustainable development of the sharing economy. This requires higher and consistent verifying standards in the filtering and screening of the identity of the provider, and the quality of products or assets.

This document aims to:

— fill in the lack of market access systems related to the sharing economy, improve the qualifications for entry into the sharing economy digital platform, and promote the healthy and sustainable development of the sharing economy;

— effectively define the main responsibilities of platform operators, ensure that platform operators build a reasonable verification mechanism to assess the specific qualifications of providers;

— clarify the access conditions for providers of the sharing economy platform, promote the transparency of providers' information, the safe and reliable platform operation, and provide guidance for the platform operator to formulate internal platform entry standards;

— protect the interests of consumers, and promote the establishment of a mutual trust mechanism between providers, platform operators, and users.

Sharing economy — Guidance for provider verification on digital platforms

1 Scope

This document provides guidelines for sharing economy platform operators when verifying providers, including on-boarding, maintenance, and deactivation.

This document applies to both digital platform operators and providers within the sharing economy.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 42500, *Sharing economy — General principles*

ISO/TS 42501, *Sharing economy — General trustworthiness and safety requirements for digital platforms*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 42500 and the following 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
identity
information or documents validating who an individual or organization claims to be

3.2
background
information originally collected or held by public authorities that is notably related to records of criminal convictions or arrests

3.3
qualifications
ability to provide products or assets reliably and consistently with specific principles

Note 1 to entry: The principles are given in Clause 4.

4 Specific principles for verification

4.1 General

In additional to the general principles in ISO 42500 and the general requirements in ISO/TS 42501, the following additional specific principles should be followed by the platform operator when verifying the provider's information and how provider activities on the platform are conducted.

a)   protection of intellectual property;

b) protection of security and privacy;

c) efficiency;

d) continual improvement.

4.2 Protection of intellectual property

In addition to the requirements set out in ISO/TS 42501:2022, 6.3.3, the platform operator should be aware of intellectual property protection laws, closely cooperate with intellectual property owners and protect intellectual property rights. The platform operator should specify in their terms of use that infringement of intellectual property rights by the provider (or the user) is prohibited.

4.3 Protection of security and privacy

In addition to the requirements set out in ISO/TS 42501:2022, 6.6.1, 6.6.2 and 6.6.15, the platform operator should establish mechanisms to maintain the security and privacy of information security in all phases of its operation, including during the verification process and process only the required personal data and information. The platform operator should treat personal information with confidentiality confidentially, and observe the privacy of providers and users, especially with regard to the collection, use, storage and disclosure of personal information.

4.4 Efficiency

In addition to the requirements set out in ISO/TS 42501:2022, 6.5.6, the platform operator should develop viable technical verification mechanisms that balance the desired user experience in a timely manner with the proper verification process to prevent entry to the platform by suspicious or confirmed fraudulent actors.

4.5 Continual improvement

The platform operator's processes should include means for continuous improvement in meeting the needs and interests of the provider and user based on the following factors.

a) feedback from interested parties;

b) evolving laws and standards.

5 Provider on-boarding by platform operator

5.1 General

The general process of provider on-boarding by the platform operator involves the following steps.

a) the provider applies to enter the platform;

b) the provider agrees to the terms of use and data and privacy statements;

c) the platform operator confirm that the provider applicant has met the eligibility criteria. The platform operator may enlist outsourcing vendors to access public records databases as part of this process;

d) in addition to the requirements set out in ISO/TS 42501:2022, 6.4.1, the platform operator informs the provider applicant of approval or declination on to the platform;

e) on the basis of the foregoing conclusion, the provider is then either approved onto the platform, e.g. are on- boarded by the platform operator, or declined from the platform operator.

Consistent with the principle of accountability, the platform operator should consult objective resources (including insurance claims) and establish procedures for assessing the risk arising from the products and assets made available on the platform, as well as from their relative diversification or concentration.

In addition to the requirements set out in ISO/TS 42501:2022, 6.2.3, the platform operator should consider these risks in the establishment of its acceptance or on-boarding criteria. Where the associated risks to public health and safety require higher levels of skills or heightened assurances of identity and background, the platform operator may impose additional or more stringent acceptance criteria. However, the platform operator should also consider the availability of reliable information to provide these assurances. In addition to the requirements set out in ISO/TS 42501:2022, 6.2.3, in all instances, the platform operator should request documentation, which, if authentic would suffice to prove the identity of the applying provider.

In addition to the requirements set out in ISO/TS 42501:2022, 6.2.3 and 6.4.5, the platform operator should verify the identity, background and capability of providers to a degree commensurate with the level of risk associated with their operations, such as: where the operations of platform operators necessitate providers and users physically meeting, there needs to be more stringent verification mechanisms in place.

5.2 Account creation and application for entry to the platform

When platform operator apply to enter the platform, they should also submit any relevant supporting documentation requested through the platform as part of acceptance criteria and described in the platform's terms of use.

Providers should submit the documents and relevant certificates required for entering the platform, which are specified in 5.3, and then wait for the platform operator to verify their submission.

NOTE   The platform operator can use technical resources to enable the provider to import providers' data from another digital platform engaged in substantially comparable activity.

5.3 Acceptance or rejection of providers onto platform

5.3.1 General

The platform operator should have a mechanism to systematically authenticate the credential submitted by the provider to ensure that the submitting provider has access to the information device associated with the mobile phone number, the email address or social media account.

The platform operator should request providers to submit government-issued proof of identification in the case of individuals and proof of establishment as an authorized for-profit or not-for-profit entity in the case of organizations.

NOTE 1   The platform operator can verify identity through email, mobile phone number, social media account and advanced technology. The advanced technology can be the password, ID badge, cryptographic key, fingerprint and other biometric data authentication.

Once submitted by the provider, the platform should have a procedure or mechanism to confirm that the documentation meets the acceptance criteria established and made available to the provider in the platform's terms of use. As part of the on-boarding process, the platform operator may use outsourcing vendors to access public records databases to conduct background checks, driver and motor vehicle records, and other verifications based on relevant information collected and maintained by public authorities and made available to requesters in accordance with local laws.

Consistent with the principle of continual improvement, the platform operator should seek to establish effective means of confirming that any credentials are current and valid, as well as facilitating the users' ability to assess providers' qualifications to meet their needs.

NOTE 2   Where there is a requirement to verify the age of a provider, BS/PAS 1296:2018 can be used.

5.3.2 Identity

In addition to the requirements set out in ISO/TS 42501:2022, 6.2.3, the platform operator should authenticate the provider's account or digital credentials. If such credentials are not valid, the provider should not be allowed to be registered onto the platform or pursue the entry process.

a) in addition to the requirements set out in ISO/TS 42501:2022, 6.5.4, the platform operator should systematically request providers to identify themselves as an organization or an individual. If the provider is an individual, the platform operator should systematically request an electronic copy of the provider's government-issued identification, such as a driver's license, passport, or national identity card. Similarly, for other assets whose provision would require a license or permit to provide them, the platform operator should systematically request a digital copy of the license or permit and verify that the document is current;

b) if the provider is an organization, the platform operator should systematically request documentation establishing the organization's existence and ability to conduct business in its names, such as certificates or articles of incorporation, business license, organization code certificate, etc., and the identity of the legally authorized representative of the company.

5.3.3 Background

The platform operator should put in place a dynamic or rolling background check mechanism. At a minimum, the platform operator should ensure that it meets its on-boarding criteria set forth in its terms of use.

If the provider is an individual, the platform operator should verify only the necessary background information which could impact the products or asset exchange while respecting privacy.

5.3.4 Capability

If the provider is an individual, the platform operator should assess the capacity of the provider to provide the type of asset represented, e.g. a product.

a) where the asset is used for a service or can be converted into service, the platform operator should consider the relative skills required to perform each service hosted by the platform. The platform operator should provide guidance to both providers and users of the risks associated with insufficient skills or capability to provide the posted service. Such guidance may include referral to user reviews, explanations of the value of user ratings and reviews, and how they may be interpreted. It may also include considerations for selecting a provider or questions to ask when agreeing to provide a service. Consistent with the principle of continuous improvement, the platform operator should systematically request that providers document their right to lease the asset and establish a means of differentiating between providers that provide such documentation and those that do not. Where the service offered by the provider requires the provider to be licensed in the place the service is to be rendered, the platform operator should systematically request the provider to document the license status. The platform operator should offer the provider the means of uploading supporting documentation, and the provider may also provide links in his or her profile to free, public databases verifying the provider's good status.

b) where the asset is used for a product (or can be converted into a product) that will be leased for any duration by the provider to the user, the platform operator should establish mechanisms or procedures to reduce the risk of the asset being leased without the provider having the legal right or authority to do so. At a minimum, the platform operator should require more than one photograph of the asset with information of the time when the photograph was taken to be uploaded to the platform. Ideally, and consistent with the principle of continuous improvement, the platform operator should systematically request that providers document their right or authority to lease the asset, and the platform operator should establish a means of differentiating between providers that provide such documentation and those that do not. Where the product to be leased requires routine maintenance to function appropriately and safely, the platform operator should likewise request that providers document the servicing or maintenance of the asset and enable