International Standard

ISO 17442-3

Financial services — Legal entity identifier (LEI) —

Part 3:
Verifiable LEIs (vLEIs)

First edition
2024-10

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 document 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 (a) patent(s) 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*.

A list of all parts in the ISO 17442 series can be found on the ISO website.

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 industry has considered issues with current digital identity tools and solutions and has devised a new approach to digital identity management. Thanks to advances in distributed ledger/blockchain technology, digital identity management with the additional feature of decentralized identity verification is now possible. Based on a concept known as "self-sovereign identity (SSI)", this new approach for authentication and verification of digital identity began as a means by which a person, the identity holder, has control of their personal data over how, when and to whom those data are revealed. This approach is set to transform the nature of identity management and how person-to-entity, or entity-to-entity, interactions take place in the digital world. It can address the need for automation in verification while maintaining data privacy and confidentiality.

The legal entity identifier (LEI) plays a key role in this process. So, the Global Legal Entity Identifier Foundation (GLEIF), manager of the Global LEI System in which the ISO 17442 series has been implemented, continues its work so that each business worldwide has only one global identity and this includes a digital identity by expanding the ISO 17442 series. This document is dedicated to leveraging the LEI in digitally signed credentials that are not only tamper-resistant but capable of being verified in a decentralized manner. Chaining of the verifiable legal entity identifier (vLEI) credentials in the vLEI trust chain using authentic chained data container (ACDC) credentials allows for the provenance of vLEIs to be traced back to GLEIF as both the root of trust for the vLEI trust chain as well as to the entity, under regulatory oversight, that ensures the operational integrity of the global LEI system.

This document enables LEIs to be used in both the recent innovation of credentials based on decentralized digital identity as well as X.509 public key certificates as outlined in ISO 17442-2.

As with standard X.509 digital certificates, vLEIs will use ISO 5009. Combining LEIs with official organizational roles is a key enabler for digital identity management for organizations and persons acting on behalf of organizations.

Financial services — Legal entity identifier (LEI) —

Part 3:
Verifiable LEIs (vLEIs)

1 Scope

This document specifies the use of the legal entity identifier (LEI) code, represented in ISO 17442-1, in authentic chained data container (ACDC) credentials.

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 17442-1:2020, *Financial services — Legal entity identifier (LEI) — Part 1: Assignment*

ISO 5009:2022, *Financial services — Official organizational roles — Scheme for official organizational roles*

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
official organizational role
official role of a person within an organization or legal entity within a particular jurisdiction that is publicly discoverable in formation, registration or other official documents of the organization or legal entity

Note 1 to entry: The scope of official organizational roles used within the verifiable legal entity identifier credentials includes, but is not limited to, the official organizational roles assigned according to ISO 5009.

3.2
legal entity
legal person or structure that is organized under the laws of any jurisdiction

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

3.3
authentic chained data container credentials
ACDC credentials
type of verifiable credential that includes the feature of normative support for chaining of credentials and relies on a suite of other technical specifications including the Key Event Receipt Infrastructure specification and the Composable Event Streaming Representation specification

3.4
verifiable legal entity identifier
verifiable LEI
vLEI
authentic chained data container (3.3) credential which contains an LEI issued in accordance with the vLEI Ecosystem Governance Framework requirements

3.5
qualified verifiable legal entity identifier issuer
qualified vLEI issuer
QVI
organization that has been qualified by the Global Legal Entity Identifier Foundation to issue and revoke verifiable LEIs

4 Governance of the vLEI ecosystem and infrastructure

The governance of the vLEI ecosystem and infrastructure is set forth in the verifiable LEI (vLEI) Ecosystem Governance Framework, which has been developed using the Trust over IP Foundation Ecosystem Governance Framework metamodel. The Global Legal Entity Identifier Foundation (GLEIF) is the governing authority for the vLEI ecosystem and infrastructure and is responsible for maintaining the vLEI Ecosystem Governance Framework.

The complete vLEI Ecosystem Governance Framework can be accessed via Reference [4].

GLEIF has established itself as the root of trust for the vLEI ecosystem and infrastructure by issuing a root autonomic identifier (AID) which anchors the cryptographic chain that will be formed by the ACDC chained credentials. The ACDC specification can be accessed via Reference [2].

GLEIF has also issued the delegated AIDs that allow GLEIF to be able to issue vLEIs to a network of trusted partners that GLEIF will qualify to issue vLEI entity level and role credentials to legal entities which identify persons acting on behalf of a legal entity and the official or functional roles in which these persons represent the legal entity.

5 vLEI credentials

The vLEI credentials shall be composed of three general categories: entity credentials, role credentials and authorization credentials:

— An entity level vLEI credential enables the identification of a legal entity by means of its LEI and enables the LEI to be authenticated as owned by a particular legal entity by means of the decentralized verification capabilities of ACDC credentials. The qualified vLEI issuer vLEI credential and the legal entity vLEI credential are entity credentials.

— A role vLEI credential specifies the relationship or context in which a person represents a legal entity either officially or functionally. Role credentials were designed since legal entities do not act on their own; people represent legal entities and act on their behalf. In these credentials, the organization represented by its LEI is specified along with the identification of a person, e.g. the name of a person, and the role in which that person represents the legal entity. The legal entity official organizational role vLEI credential and legal entity engagement context role vLEI credential are role credentials.

— Finally, the qualified vLEI issuer authorization vLEI credential is an authorization credential.

All vLEI credentials shall contain LEIs which have been assigned in accordance with ISO 17442-1.

In this document, vLEI credential types are defined as follows. Other credential types may be defined.

a) Qualified vLEI issuer vLEI credential
An entity credential issued by GLEIF to a qualified vLEI issuer, an organization that has been qualified by GLEIF to issue and revoke certain vLEI credentials to legal entities and persons acting on behalf of a

legal entity in either official or functional roles. A qualified vLEI issuer vLEI credential contains the LEI of the qualified vLEI issuer.

b) Legal entity vLEI credential
An entity credential issued to a legal entity which has contracted with a qualified vLEI issuer to issue vLEI credentials. A legal entity vLEI credential can be issued only by qualified vLEI issuers. A legal entity vLEI credential contains the LEI of the legal entity.

c) Legal entity official organizational role vLEI credential
A role credential issued at the request of a legal entity to a person acting on behalf of the legal entity in an official role. A legal entity official organizational role vLEI credential can be issued only by a qualified vLEI issuer. The legal entity official organizational role vLEI credential contains the LEI of the legal entity, the identification of a person, e.g. the name of the person, and the official organizational role of the person, e.g. as specified in ISO 5009. The official organizational role shall be the role specified in ISO 5009 if the official organizational role has been registered in accordance with ISO 5009.

d) Legal entity engagement context role vLEI credential
A role credential issued at the request of a legal entity to a person acting on behalf of the legal entity in a functional role. A legal entity engagement context role vLEI credential can be issued directly by a legal entity or by a qualified vLEI issuer under contract as a value-added service to a legal entity. The legal entity engagement context role vLEI credential contains the LEI of the legal entity, the identification of a person, e.g. the name of the person, and the person's functional role as specified by the legal entity.

e) Qualified vLEI issuer authorization vLEI credential
An authorization credential used by a legal entity to authorize the issuance or revocation of a legal entity official organizational role vLEI credential or a legal entity engagement context role vLEI credential (if the legal entity has contracted with the qualified vLEI issuer also to issue legal entity engagement context role vLEI credentials).
A qualified vLEI issuer authorization vLEI credential can be issued to its qualified vLEI issuer only by authorized representatives of a legal entity.

Each vLEI credential also includes additional elements that are required to be present in the schema of a vLEI credential. The schema for each vLEI credential can be accessed via Reference [5].

The requirements for each vLEI credential are specified in the credential frameworks that are part of the vLEI Ecosystem Governance Framework.

Additional data elements can be specified about a person receiving a role credential through the issuance of another ACDC credential containing these additional elements. This is accomplished by chaining the additional ACDC credential to the role credential.

6 Other features of vLEI credentials

The vLEI infrastructure is a network-of-networks of true universality and portability, developed based on the Key Event Receipt Infrastructure (KERI) protocol as the backbone of the vLEI infrastructure. The infrastructure can support the full range of blockchain, self-sovereign identity and other decentralized key management platforms. vLEIs are hostable on any infrastructure such as ledgers and cloud infrastructures. Portability also enables the vLEI ecosystem to unify all ledger-based ecosystems that support the vLEI.

A related capability called Composable Event Streaming Representation (CESR) proof signatures allows vLEIs to be used to sign individual facts, documents, taxonomies, transactions, financial messages, etc. These artefacts can be signed in their entirety as well as by specific sections/parts by one or more holders of vLEI credentials. These capabilities not only provide cryptographic verification in a decentralized manner but can also create a chain of provenance of data in the preparation, review, approval and submission of reports, for example.

The KERI and CESR specifications can be accessed via References [1] and [3].