INTERNATIONAL STANDARD

ISO 17442-2

First edition
2020-08

Financial services — Legal entity identifier (LEI) —

Part 2: Application in digital certificates

Services financiers — Schéma d'identifiant d'entité légale (IEL) —

Partie 2: Utilisation dans les certificats numériques

Reference number
ISO 17442-2:2020(E)

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

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 68, *Financial services*, Subcommittee SC 8, *Reference data for financial services*.

This first edition of ISO 17442-2, along with ISO 17442-1, cancels and replaces ISO 17442:2019, which has been technically revised.

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

Legal entity identification is an integrated and necessary component of financial transactions. Entering into business relationships requires "know your customer" processes to be initiated and maintained for the duration of these relationships and any longer-term data retention requirements to be addressed. Parties involved in financial transactions need to be identified in the records of these transactions. Then the risk for each party and the resulting concentration risk need to be measured. All of this needs to be achieved while the support for straight through processing (STP) is maintained.

Both legal entity identifiers (LEIs) and digital certificates are established tools for identity management. These tools can be of even greater benefit to users if they are combined so that they complement each other, providing a new solution to standardized digital identity. Annex B outlines the mutual benefits of this combination.

It is possible, for example, to display the LEI in a web browser address bar from the digital certificate or retrieve information from the LEI data record using an application programming interface (API).

Furthermore, the public key certificate can be linked to the LEI and its associated data record.

Financial services — Legal entity identifier (LEI) —

Part 2:
Application in digital certificates

1 Scope

This document specifies a standardised way of embedding the legal entity identifier (LEI) code, as represented in ISO 17442-1, in digital certificates, represented by the International Telecommunications Union (ITU) Recommendation X.509 and its ISO equivalent standard, ISO/IEC 9594-8.

This document specifies the structure of a public key certificate conforming with ISO/IEC 9594-8 in which the LEI is embedded.

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 terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
LEI data record
set of data attributes associated with the legal entity identifier (LEI)

Note 1 to entry: See ISO 17442-1:2020, Clause 6.

3.2
object identifier
OID
ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node

[SOURCE: ISO/IEC 9834-1:2012, 3.5.11]

4 Structure of the X.509 public key certificate with embedded LEI

Embedding the LEI into digital certificates should be achieved by leveraging an object identifier (OID) to place the LEI in the public key certificate. The OID 1.3.6.1.4.1.52266.1 has been registered for this purpose.

In cases in which the role of the individual named in the digital certificate should be indicated, the optional element of role can be added to the digital certificate. For this purpose, OID 1.3.6.1.4.1.52266.2 (role) has been registered.

Thus, there are defined places for LEI and the role of the individual in public key certificates.

These OIDs for the LEI and the role will be included as specific extensions. The extension ASN.1 type is defined in ISO/IEC 9594-8:2017, 7.2 as:

```
Extension ::= SEQUENCE {
      extnId    EXTENSION.&id({ExtensionSet}),
      critical    BOOLEAN DEFAULT FALSE,
      extnValue    OCTET STRING
       (CONTAINING EXTENSION.&ExtnType({ExtensionSet}{@extnId})
      ENCODED BY der),
      ... }
der OBJECT IDENTIFIER ::=
   {joint-iso-itu-t asn1(1) ber-derived(2) distinguished-encoding(1)}
```

The component `extnId` is the OID. The component `critical` may be set to `FALSE`. The component `extnValue` is some type which contains the LEI code.

The LEI and role extensions are defined respectively as:

```
leiExtension      EXTENSION ::= {
      SYNTAX  PrintableString(SIZE(20))
      IDENTIFIED BY lei}
Lei   OBJECT IDENTIFIER ::= {1 3 6 1 4 1 52266 1}
roleExtension      EXTENSION ::= {
   SYNTAX PrintableString(SIZE(1.. ub-leiRole-length))
   IDENTIFIED BY role}
Role   OBJECT IDENTIFIER ::= {1 3 6 1 4 1 52266 2}
```

An illustration of a digital certificate prepared in accordance with this document is provided in Annex A.

Annex A
(informative)

Example digital certificate with embedded LEI and role

An example digital certificate representing the CEO of an entity with the LEI YZ83GD8L7GG84979J516 and conforming to ITU Recommendation X.509 and ISO/IEC 9594-8 might be visualised as follows.

NOTE "#####" represents different values that have been made anonymous for the purposes of this example.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: #####
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=#####, O=#####, OU=#####, CN=#####
        Validity
            Not Before: Jan  1 00:00:00 2019 GMT
            Not After : Jan  1 00:00:00 2022 GMT
        Subject: C=#####, L=#####, O=#####, CN=#####
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit): #####
                Exponent: #####
        X509v3 extensions:
            X509v3 Subject Key Identifier: #####
            X509v3 Basic Constraints: critical
                CA:#####
            X509v3 Authority Key Identifier: #####

            qcStatements: #####
            X509v3 Certificate Policies: #####
                  User Notice: #####

            X509v3 CRL Distribution Points: #####

            X509v3 Key Usage: critical
                #####
            X509v3 Extended Key Usage: #####
            1.3.6.1.4.1.52266.1: YZ83GD8L7GG84979J516
            1.3.6.1.4.1.52266.2: CEO
    Signature Algorithm: sha256WithRSAEncryption
        #####
-----BEGIN CERTIFICATE-----
#####
-----END CERTIFICATE-----
```