
**Security and resilience — Authenticity,
integrity and trust for products
and documents — Guidelines to
establish a framework for trust and
interoperability**

*Sécurité et résilience — Authenticité, intégrité et confiance pour les
produits et les documents — Lignes directrices visant à établir un
cadre pour la confiance et l'interopérabilité*

iTeh STANDARDS (standards.iteh.ai)

[ISO 22385:2023](https://standards.iteh.ai/catalog/standards/sist/e2fab48b-bfc9-492b-9fb1-e0c6bd5aa1d6/iso-22385-2023)

<https://standards.iteh.ai/catalog/standards/sist/e2fab48b-bfc9-492b-9fb1-e0c6bd5aa1d6/iso-22385-2023>



iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 22385:2023

<https://standards.iteh.ai/catalog/standards/sist/e2fab48b-bfc9-492b-9fb1-e0c6bd5aa1d6/iso-22385-2023>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2023

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.....	iv
Introduction.....	v
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	1
4 Scheme governance document.....	2
5 Recommendations applying to the actors of the ESEDS scheme.....	3
6 Organizational measures.....	3
7 Technical measures.....	3
8 Internal scheme resources.....	3
9 Directories.....	4
Annex A (informative) Example of an ESEDS.....	5
Annex B (informative) Example of a visible digital seal scheme for each directory.....	10
Bibliography.....	15

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 22385:2023

<https://standards.iteh.ai/catalog/standards/sist/e2fab48b-bfc9-492b-9fb1-e0c6bd5aa1d6/iso-22385-2023>

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 292, *Security and resilience*.

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

Creating trust, interoperability and interoperation in the digital world is vital. To mitigate the damage resulting from counterfeited physical and electronic documents, products, software and services, it is necessary to consider both physical and digital security layers.

Electronically signed encoded data set (ESEDS) schemes can be used to deter counterfeiting when anyone along the supply chain, including distributors, independent brokers, law enforcement agents and end customers, can use them to access a secure local or remote description of a product or a document. A common and unique mechanism of data integrity check applied to various specific and individual items or to unique resource identifiers (URIs) can contribute to early detection of counterfeits.

This document, applicable to ESEDS schemes, is intended to enable reliable and safe product (hardware, software, services, etc.) authentication and traceability processes by describing the necessary trusted environment. This will support interoperation of trusted services by realizing marking and monitoring mechanisms along the products' and documents' value chain.

The proposed ESEDS scheme is intended to remain as a totally voluntary scheme, that is independent from other authentication and track and trace systems.

The use of ESEDS to access trustful data from a local or remote source give end users and law enforcement agents powerful tool to detect counterfeits and mitigate the risk of being exposed to counterfeited products and documents.

The ESEDS uses the electronic signature capacity that is used to verify the integrity of the of the data and to identify/authenticate the manufacturer/issuer of the product or document on which the ESEDS is placed. The verification can be performed online or off-line, utilizing the functions supported by the signed use case descriptor file ("manifest").

The ESEDS can take the form of two different media or any combination:

- printed on a physical product or any physical document,
- as a set of electronic data and/or as displayed and read as a machine-readable code (MRC).

Implementation of these guidelines allows different market sectors and market actors to share the same global ESEDS scheme architecture and semantic, actor definition and associated processes. This way a sector interoperability and a global cross-interoperation can be achieved.

Fighting against physical and electronic documents, products, software and services fraud within the supply chain is a key challenge. The fraud issues heavily impact subcontractors, partners and suppliers. In parallel, more and more national and international regulations are requesting a full "back-to-back liability" such as Product Liability Directive in United States of America and Europe as well as General Data Protection Regulation (GDPR) in the European Union (EU).

The creation of trust and interoperability will facilitate such liability conformity via the usage of an ESEDS. It will help to correctly understand a UID of any particular manufacturer/provider for a given product, sub-product, software and services across different market sectors. Interoperable online and/or off-line identification and authenticity check of the product, document, software or services will become possible to put in place.

This implies that all actors from different market sectors have the same understanding of the complete ESEDS scheme, its governance model and its documentation hierarchy and structure.

The global scheme is summarized in the flow-chart in [Figure 1](#).

ESEDS scheme: Framework for trust and interoperability

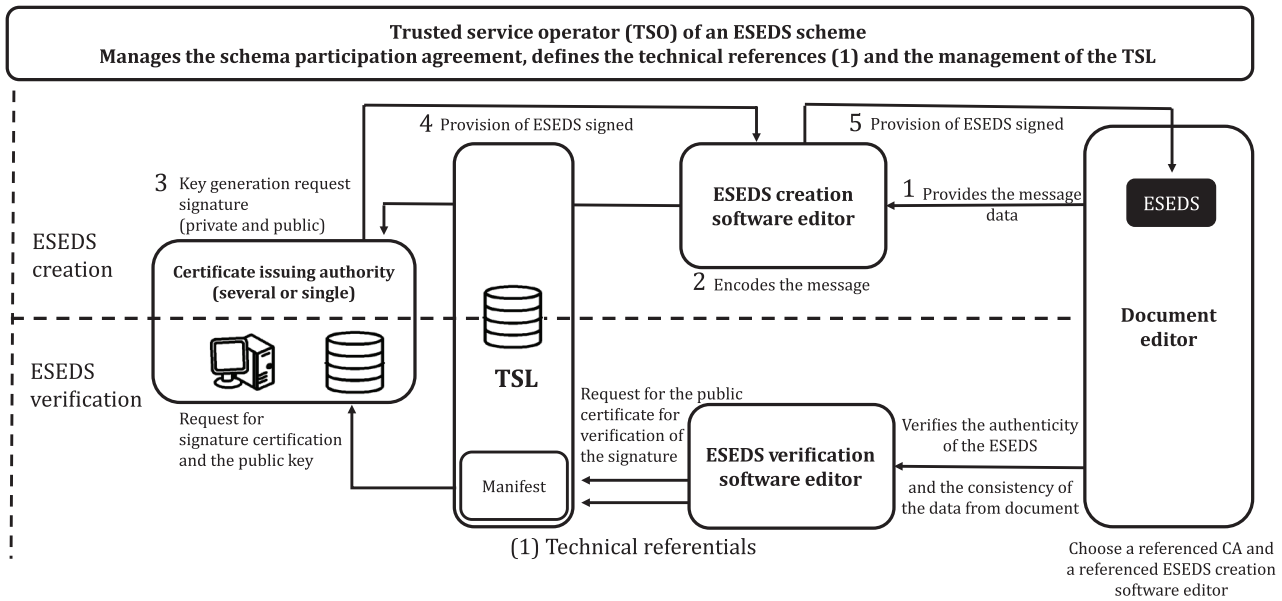


Figure 1 — ESEDS Scheme

This document contains the following elements to be considered to design a reliable and trustful ESEDS:

- fundamental document of the scheme (see [Clause 4](#));
- recommendations applying to the actors of the scheme (see [Clause 5](#));
- organizational measures (see [Clause 6](#));
- technical measures (see [Clause 7](#));
- internal scheme resources (see [Clause 8](#));
- directories (see [Clause 9](#)).

These clauses are the essential elements of an ESEDS scheme governance model. Each clause is constituted by one or several documents that are describing the mandatory elements to be produced by different ESEDS scheme actors.

All essential elements of ESEDS scheme are presented as a hierarchy in [Figure 2](#).

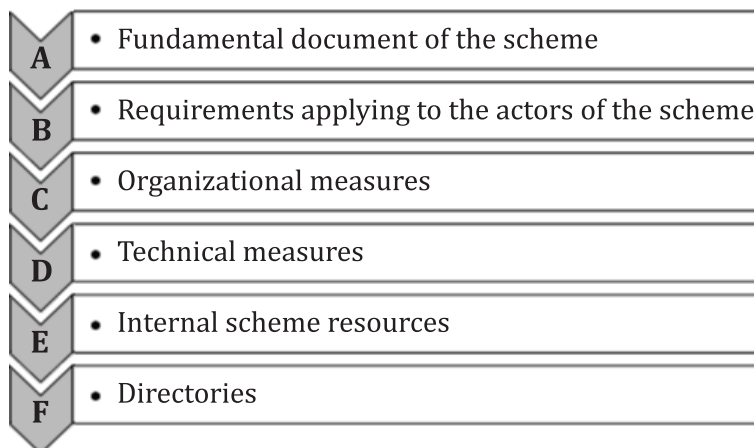


Figure 2 — ESEDS essential elements

The ESEDS model proposed by this document can be applied by multiple independent certification authorities (CAs), in contrast to the International Civil Aviation Organization (ICAO) model which concerns solely multinational parent/daughter hierarchical CAs. The organization of the trust environment proposed by this document therefore allows for both hierarchical CA models (such as ICAO) and sectoral, national or international models based on multi-sectoral CAs to cooperate. Based on this approach, a universal reader application (trusted entry point, TEP) that is agnostic to any use case can be developed provided that common data structures are used. The ESEDS system can be considered as a potential global trust environment if the rules and principles of this document are followed. Ultimately, interoperability between independent trust service operator (TSO) trust networks can be achieved by using the same common data structures, based on appropriate standards and specifications, and by mutual recognition of their respective ESEDS schemes.

This document is applicable to developers and users of secure and interoperable identification systems. It is open for any industry and is technology agnostic and does not interfere with existing identification, track and trace, and authentication systems but is able to introduce an interaction between them.

This document is part of a family of standards which includes ISO 22380, ISO 22381, ISO 22382, ISO 22383 and ISO 22384.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO 22385:2023](https://standards.iteh.ai/catalog/standards/sist/e2fab48b-bfc9-492b-9fb1-e0c6bd5aa1d6/iso-22385-2023)

<https://standards.iteh.ai/catalog/standards/sist/e2fab48b-bfc9-492b-9fb1-e0c6bd5aa1d6/iso-22385-2023>

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines to establish a framework for trust and interoperability

1 Scope

This document establishes a framework for a trustworthy environment for information processing and communication that protects integrity along the supply chain of physical and related electronic documents, products, software and services life cycle to mitigate product fraud and counterfeit goods, by using object identification techniques.

This document gives guidelines to establish a framework for ensuring trust, interoperability and interoperation via secure and reliable electronically signed encoded data set (ESEDS) schemes for multi-actor applications which are even applicable in multi-sector environment.

This document does not interfere with existing traceability and identification and authentication systems but is able to support interoperations between them by introducing an ESEDS scheme.

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 22300, *Security and resilience — Vocabulary*

<https://standards.iteh.ai/catalog/standards/sist/e2fab48b-bfc9-492b-9fb1-e0c6bd5aa1d6/iso-22385-2023>

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 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

electronically signed encoded data set

ESEDS

structured data set containing the header, payload, signature and optional auxiliary data block

Note 1 to entry: The payload type and issuer identity are included in the header.

Note 2 to entry: ESEDS can often be expressed as *machine-readable code* (3.3).

3.2

trust service operator

TSO

legal entity that is the unique owner of the complete *electronically signed encoded data set (ESEDS)* (3.1) scheme and fulfils three roles:

- manage the trust service list
- manage the manifest

- provide the operating governance rules of the ESEDS scheme

3.3 machine-readable code

MRC

graphic symbol or electronic device, or a combination of the two, containing a set of signs or letters that can be interpreted by an acquisition system

Note 1 to entry: Examples of MRC include, but are not limited to, 2D barcodes and radio frequency identification (RFID) tags.

3.4 trusted entry point

TEP

method provided and/or certified by the *trust service operator* (3.2) having support for the response formatting function (RFF) and open for additional object identification and authentication systems (OIAS) able to resolve without ambiguity any unique identifier (UID)

3.5 trust service list

TSL

list containing compliant information about the *trust service operator* (3.2), the trust service providers (TSPs) and the TSP's certificate authority (CA) authorized to issue certificates to sign *electronically signed encoded data sets* (3.2)

Note 1 to entry: ETSI TS 119 612 sets out what is a compliant TSL.

Note 2 to entry: TSLs are extensible using extensible markup language (XML) defined by the *trust service operator* (3.2).

3.6 trust service provider

TSP

legal entities participating in an *electronically signed encoded data set (ESEDS)* (3.1) scheme providing several functions or trust services such as:

- electronic certificate
- electronic signature
- time stamping
- any other trust services related to the ESEDS scheme requirements

3.7 back-to-back liability

full transfer of liability from the contractor to the subcontractors

3.8 manifest

use case manifest

external resource containing information in an XML format related to each single *electronically signed encoded data set* (3.1) use case, its data schema, validation policies and optional extensions

4 Scheme governance document

The fundamental scheme governance document is created by the TSO.

It should be accepted by all the actors as the reference for the ESEDS scheme governance model.

It is a scheme in which actors agree to be bound by governance.

The governance document provides the main principles to describe the essential elements to be present and listed into the membership contract to participate in the ESEDS scheme.

The objective is to define the roles, responsibilities and obligations of the players in the ESEDS scheme.

5 Recommendations applying to the actors of the ESEDS scheme

The ESEDS scheme, as defined by the TSO, should include five technical specifications (TS) which impact the participating actors, as follows:

- TS 1: Technical measures specifying how the TSOs of an ESEDS scheme ensure confidence in the TSOs of the ESEDS scheme.
- TS 2: Technical measures specifying how the trust service providers (TSPs) guarantee the consistency of the service level of the TSPs of the ESEDS scheme.
- TS 3: Technical measures specifying how the ESEDS creation systems ensure interoperability.
- TS 4: Technical measures specifying how the ESEDS verification software ensures interoperability.
- TS 5: Technical measures specifying how the document publisher ensures interoperability.

6 Organizational measures

The ESEDS scheme, as defined by the TSO, should include a dedicated document that describes the life cycle management process that all the actors and participants follow.

This document shall be used by all ESEDS scheme actors. It is a key measure to guarantee the smooth usage of the ESEDS scheme.

7 Technical measures

The ESEDS scheme, as defined by the TSO, may follow other standards or specifications that include technical measures describing the data organization for the use of an ESEDS or comparable data structures.

EXAMPLE ISO/IEC 20248:2022 or AFNOR XP Z42-105:2019 for the authentication, verification and acquisition of data carried by a document or object.

[Annex A](#) gives an example of an ESEDS.

8 Internal scheme resources

The ESEDS scheme, as defined by the TSO, should include the following internal scheme resources:

- A trust service list (TSL) that needs to be publicly reachable and machine-readable. The objective is that the list of TSPs is publicly available.
- A manifest providing a necessary input and mechanism which allows the scheme applicability towards different trust services, data presentation and off-line verification.

These two internal scheme resources should be described in two separate technical specifications.