INTERNATIONAL STANDARD

ISO 22385

First edition
2023-02

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

Reference number
ISO 22385:2023(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 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.

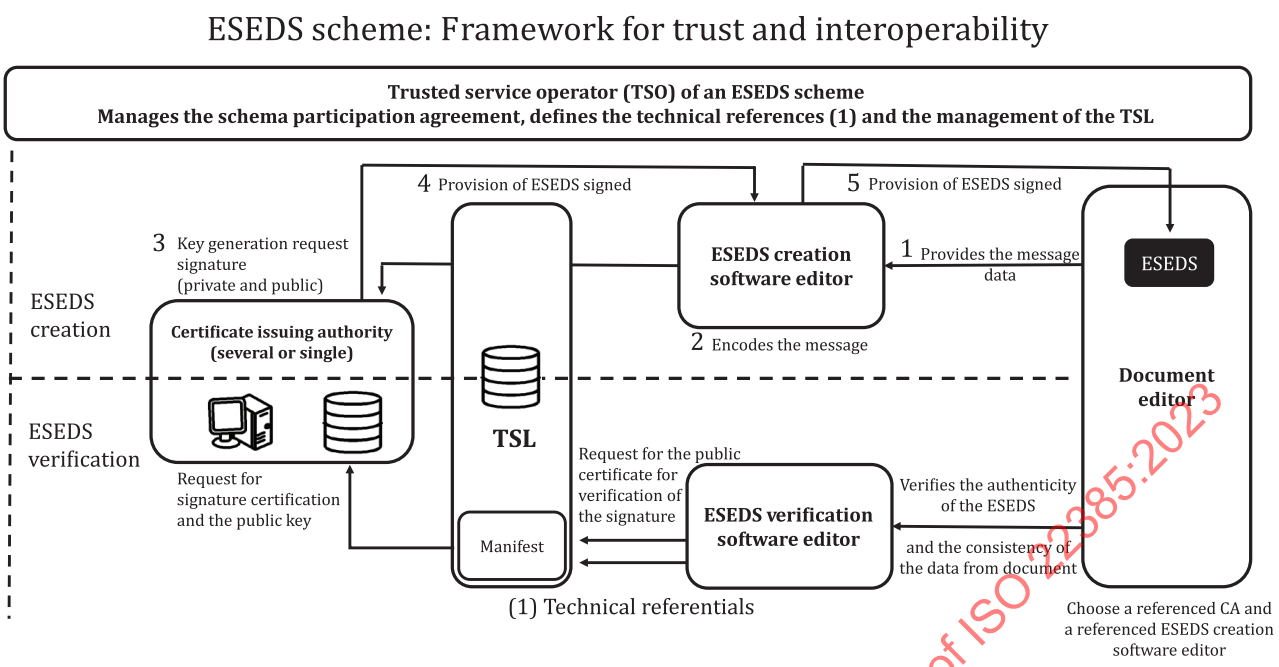

Figure 1 — ESEDS Scheme

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.

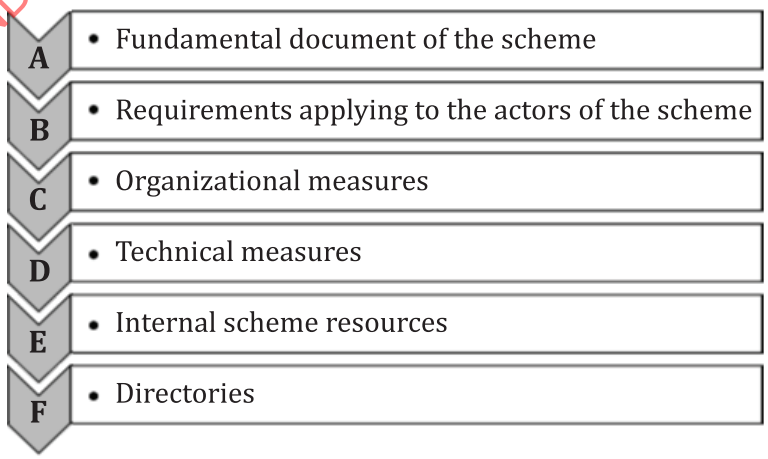

Figure 2 — ESEDS essential elements

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.

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*

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.

9 Directories

The ESEDS scheme, as defined by the TSO, should have four different directories that are essential for the global ESEDS scheme interoperability. The directories should include the following information:

— Directory number 1: List of participants, which allows verification of the validity of the agreements to join the ESEDS scheme.

— Directory number 2: List of TSPs qualified by the scheme, which allows verification of the validity of the agreements to join the ESEDS scheme.

— Directory number 3: List of the ESEDS software creation editors, which allows verification of the validity of the agreements to join the ESEDS scheme.

— Directory number 4: List of ESEDS software verification editors, which allows verification of the validity of the agreements to join the ESEDS scheme.

Annex B gives an example of a visible digital seal (VDS) scheme for each directory.

Annex A
(informative)

Example of an ESEDS

A.1 General

A common example of an ESEDS is the VDS. The VDS consists of embedding in a 2D barcode the essential information of an object, which can be a document, security label or a security plate, see the example given in Clause A.2 for semiconductors. This information is locked by an electronic signature of the hash of these data, which guarantees the identification of the issuing organization and the integrity of the object. The data of the 2D code are electronically signed by the private key corresponding to a public key placed in an electronic seal certificate X.509. This asymmetrical encryption allows the control of the signature by all the actors of the supply chain with the public key of the issuing signing party. The delivery of this electronic certificate is controlled by the TSO who verifies the rights of the VDS issuer in relation to the document. The signature is performed by the TSP that generates the electronic seal. The signature is verified by any entity via a TEP. If the signature of the data is correct, this indicates that these data (and only these data) are correct. Such data can be used as trustful input data for a new application or another use case.

Use cases examples are given in Clauses A.2 to A.7.

A.2 Use case: Semiconductors

Figure A.1 shows the structure of an ESEDS for semiconductors.

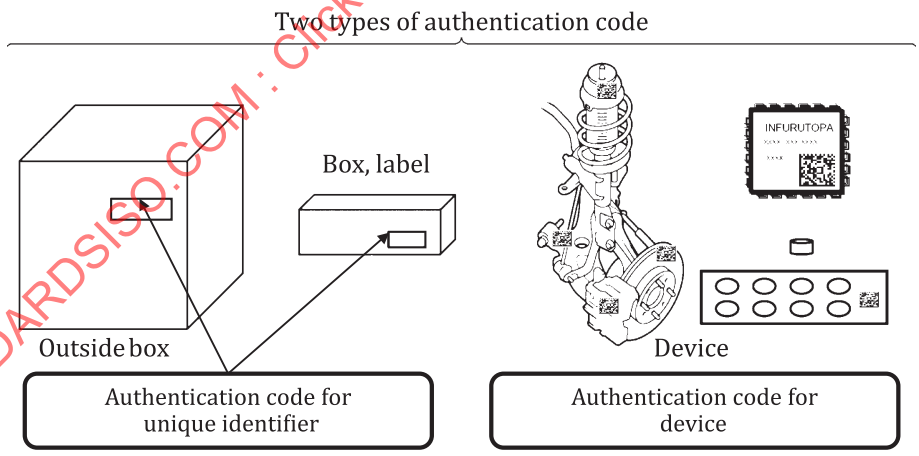

Figure A.1 — General format of an ESEDS for semiconductors

The following example shows the format and content of the authentication codes issued or registered by a specific authentication body (the equivalent of a TSP in the ESEDS scheme) for devices and unique identifiers:

a) Identifier: Refer to the following:

NOTE The following documents are for the field of semiconductors.

— ISO/IEC 15418:

— automatic identification and data capture techniques;

  - GS1 application identifiers and ASC MH10 data identifiers and maintenance;
- ISO/IEC 15434:
  - automatic identification and data capture techniques;
  - syntax for high-capacity ADC media;
- ANSI MH10.8.2:
  - data identifier and application identifier standard.

b) Unique number: Unique code to be allocated on a per unique-identifier basis.

A.3 Use case: Tax stamp

Figure A.2 shows an example of an ESEDS for a tax stamp.

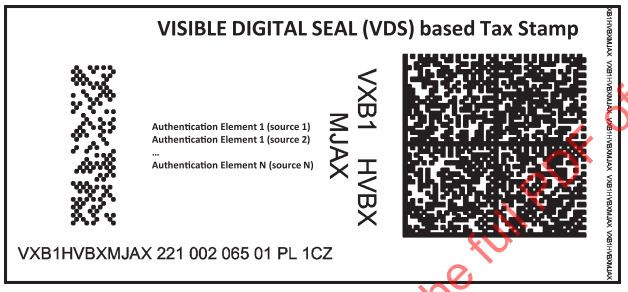

Figure A.2 — Tax stamp sample carrying an ESEDS in the large DataMatrix code based on AFNOR XP Z42-105

One method for establishing interoperability between independently functioning product identification and authentication systems, which often employ different coding architectures and different types of security features, is through the use of a VDS, which can be printed on the tax stamp in the form of a public or private 2D code.

The use of VDS is recommended by ISO 22381:2018, as a part of a TEP to allow all stakeholders (including consumers) to authenticate a unique identifier (UID) without having to go online, as well as to access information on the security features used on a particular tax stamp.

The following example explains how a VDS can be used in conjunction with a tax stamp and traceability system:

- Figure 2 shows a demo stamp carrying two different DataMatrix codes: the smaller code contains the UID to be used for unit level track and trace, and the larger code is the VDS.
- The smaller code is applied and validated during the product manufacturing process, after which a list of all validated UIDs are digitally signed by the manufacturer, who must be in possession of a qualified digital certificate issued by a TSP, and transferred to a data repository.
- The VDS code also contains the UID, as well as the UID issuer's qualified electronic signature, and a secure link to information on all security features used on the tax stamp. This enables inspectors from any member state (in the case of the EU), or even consumers, to check if the UID and other data are genuine and consistent with the product.
- The data structure is conforming to AFNOR XP Z42-105.

A.4 Use case: Internet of Things (IoT) security and safety conformity certificates

Figure A.3 shows the structure of a VDS for IoT.

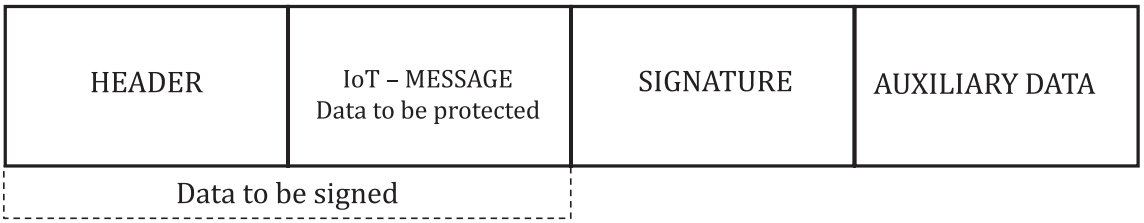

Figure A.3 — Visible digital seal for IoT

For each single item, IoT manufacturers must ensure that unique, secure and non-removable identification markings, such as engraved codes or security labels, are affixed to both the IoT device and its outside packaging.

With such a global system in place, using a single mobile application (TEP), an inspector from country A is able to securely read the VDS data issued by country B, country C or any other country being accepted by the governance body operating given ESEDS scheme.

Such a VDS also contains information and guidance on (or secure link to) the authenticating security features used by each manufacturer/country. In this way, each country is free to use different technologies and schemes, knowing that the VDS interoperability function is there to assist inspectors who are unfamiliar with some of the national schemes.

Interoperability in a trusted environment using a common TEP for various track and trace systems is an essential systemic security element. This is the condition for efficient early detection of illicit IoT items, avoiding the risk of their acceptance within the system.

A.5 Use case: Access card

Figure A.4 shows the structure of a VDS for digital identity.

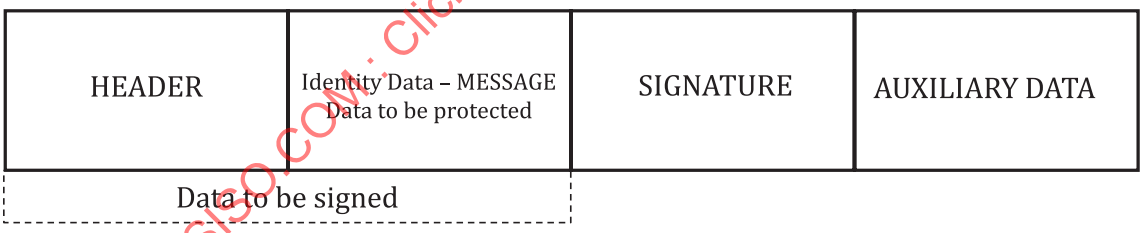

Figure A.4 — General format of visible digital seal for digital identity

Figure A.5 shows the reading sequence for a VDS digital identity basic use case.

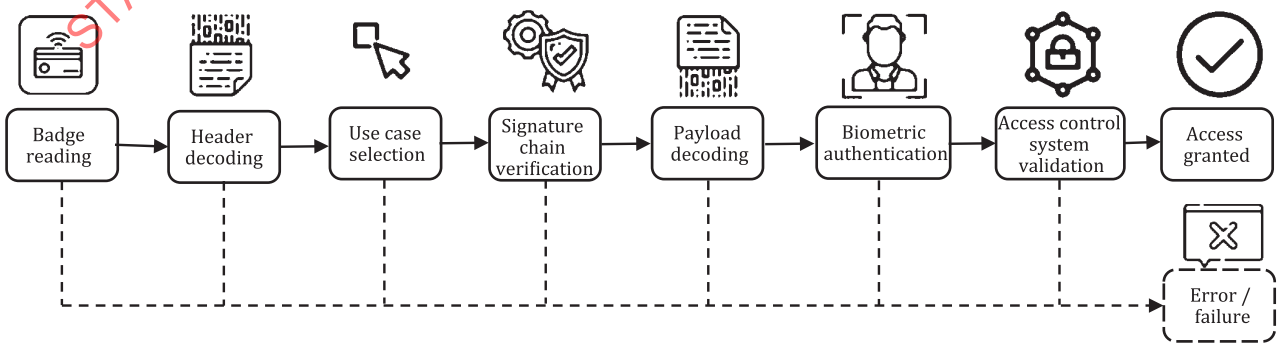

Figure A.5 — VDS-based card verification with biometric control

Digital identity is a critical domain where the issuer of the document or of the access must be trusted. Access control often involves centralized systems to manage the users, their rights and their roles related to protected zones. The access verification processes are based on personal badges, validated by unattended systems, as well as control operators to physically control the access of the zone.

Access badges must be personalized and issued by the right authority – which must be verified before an access validation.

The use of a data structure conforming to AFNOR XP Z42-105 stored in the access badges fulfils all requirements of the badge authentication. As the required authorization data (personal information as well as UID) are digitally signed by the access control system (when the badge is issued) the validation systems (electronic or human) are able to validate the origin and the authenticity of the badge.

In this case, ESEDS containing biometric templates (ID picture, fingerprints and/or face recognition pattern) can be stored as binary data in an access smart-card and/or printed under the form of a 2D barcode. When an access control is required, the validation system (TEP) reads the card, verifies the signature (electronic seal) against the trusted certificate of the issuer and proceeds to the biometric verification of the holder. Exclusively only after this verification, the access control can be granted.

A.6 Use case: ESEDS (VDS) as a know your customer (KYC) authentication service for electronic documents on blockchain or distributed ledger technology (DLT) without connection

The KYC process includes ID card verification, biometric verification and document verification (e.g. utility bills as proof of residency). It must comply with KYC regulations and anti-money laundering regulations to limit fraud.

The issuer of the document posts the hash on a blockchain. The blockchain creates a VDS containing the hash of the document and a timestamp of its delivery. The VDS is digitally signed by the blockchain.

The user collects the electronic document sent by the issuer and the VDS sent by the blockchain. The user can verify that the document sent is the one stored on the blockchain.

When a client service provider wants to verify the legitimacy of the document, he or she does not need to connect to the blockchain. The verification is performed in off-line mode with the document and the VDS which authenticates the hash necessary for this checking. Figure A.6 shows the complete process of VDS issuance and verification for a blockchain referenced document.

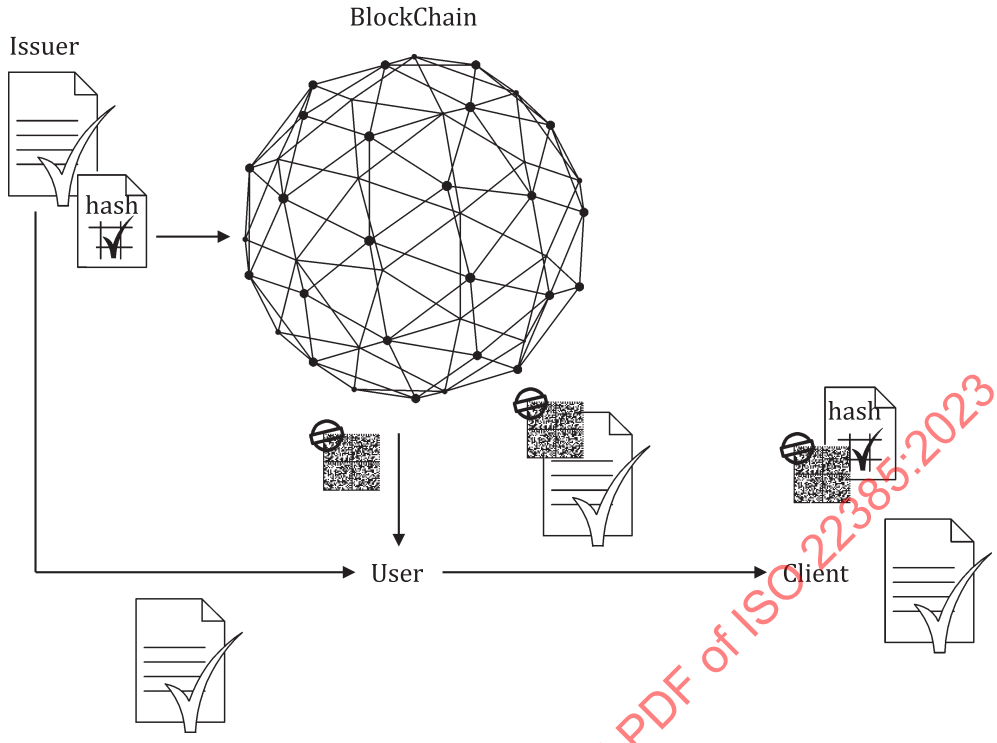

Figure A.6 — ESEDS life cycle including a proof of pre-existence

A.7 Use case: Secure payment by direct debit with an ESEDS (VDS)

The application is proposed by the customer's online bank for the payment of invoices received by email or by post mail. These invoices can also correspond to a payment on e-commerce websites.

To issue this VDS, the creditor registers with his or her bank and obtains an electronic seal certificate authorized to issue invoices. The creditor issues an invoice (paper or electronic; this can be a PDF file) on which he or she encapsulates, within a VDS, his or her bank identifier (BIC and IBAN), the invoice reference and the invoice amount.

Using an online banking application on his smartphone, the debtor can:

— authenticate the creditor;

— verify the amount of the invoice;

— initiate a payment by transfer.

The invoice reference allows the creditor to unambiguously match between the payment and the invoice. The payment operation is carried out in a single click, without having to enter the creditor's bank details.

Without VDS, the same device is likely to be attacked by falsified mails containing information referring to counterfeiters' bank accounts.

This method guarantees the security of transactions while improving ergonomics. Using existing payment schemes (direct debit or instant direct debit), it is easy to implement in online banking.

Annex B
(informative)

Example of a visible digital seal scheme for each directory

B.1 General

This annex gives an example of four directories for a VDS scheme that should be established by the TSO.

B.2 Directory 1: List of participants

(Name of visible digital seal governance body)
(Nom de l'organisme de gouvernance du cachet électronique visible)

List of participants to the governance body of visible digital seal (VDS) scheme

DIRECTORY OF PARTICIPANTS

Country	Organization registration number	Organization name	Status	Point of contact

Document history

Version	Date	Modifications	Editor
0.1	15/10/2021	Template creation	Name of editor

Comments to be sent to
Entity name / address / contact
of the governance body

Document classification : Public

B.3 Directory 2: List of TSPs of a VDS scheme

(Name of visible digital seal governance body)
(Nom de l'organisme de gouvernance du cachet électronique visible)

List of trust service providers (TSP) of visible digital seal (VDS) scheme

DIRECTORY OF TRUST SERVICE PROVIDERS

Country	Organization registration number	Organization name	Status	Point of contact

Document history

Version	Date	Modifications	Editor
0.1	15/10/2021	Template creation	Name of editor

Comments to be sent to
Entity name / address / contact
of the governance body

Document classification : Public