INTERNATIONAL STANDARD

ISO 22376

First edition
2023-08

Security and resilience — Authenticity, integrity and trust for products and documents — Specification and usage of visible digital seal (VDS) data format for authentication, verification and acquisition of data carried by a document or object

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Spécifications relatives aux formats de données et l'utilisation du Cachet Électronique Visible (CEV) aux fins d'authentification, de vérification et d'acquisition des données véhiculées par un document ou un objet

Reference number
ISO 22376:2023(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 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 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

A visible digital seal (VDS) is a presentation of a structured data set, often in the form of a machine-readable code (MRC), used to ensure the authenticity and integrity of key data associated with a document or object at a relatively low cost and with a high level of security through asymmetrical cryptography.

Systems based on a VDS format can enable enhanced and interoperable secure track and trace with related anti-counterfeiting authentication.

The trustworthiness of the data carried by a VDS is dependent on the confidence that can be granted to the certificate related to its cryptographic environment. The VDS specified in this document is one possible presentation of electronically signed encoded data sets (ESEDSs), such as, for example, uniform resource identifier (URI) formatted in accordance with GS1 Digital Link Standard and protected by digital signature in accordance with ISO/IEC 20248. The expected confidence for this VDS is provided via a related ESEDS scheme.

This document will not interfere with existing authentication, traceability and identification systems. It enables interoperability between technologically heterogenous track and trace and anti-counterfeit environments.

Implementation of a trusted entry point (TEP) is enabled, helping to reduce the number of object identification applications by combining them into a universal and use-case resilient reader for professional inspectors and consumers. This document is intended for developers and users wishing to enable secure and interoperable track and trace and authentication systems. Since the method is technology agnostic, it is available for all industrial sectors where unique identifiers (UIDs) or data need to be secured and inspected in a global and multilingual environment.

Security and resilience — Authenticity, integrity and trust for products and documents — Specification and usage of visible digital seal (VDS) data format for authentication, verification and acquisition of data carried by a document or object

1 Scope

This document defines the conditions necessary for the interoperable deployment of visible digital seals (VDSs). It describes the structure, possible forms of representation, production process and verification process applicable to VDSs, for any type of document or object to which they relate.

This document does not establish requirements for users that issue and verify documents or for users that implement and deploy VDSs.

This document does not apply to detailed response formatting functions (RFFs). These requirements and functions are defined by the trust service operator (TSO) and generally cover functionalities such as the security levels of certificates and governance rules to be applied to document issuers and trust service providers (TSPs) intervening in the VDS ecosystem.

This document does not apply to the governance related to the operation of the VDS scheme. It is not intended to replace the specifications from Agence Nationale des Titres Sécurisés (ANTS), Bundesamt für Sicherheit in der Informationstechnik (BSI) and International Civil Aviation Organization (ICAO) documents.

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 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country code*

ISO 14533-1, *Processes, data elements and documents in commerce, industry and administration — Long term signature — Part 1: Profiles for CMS Advanced Electronic Signatures (CAdES)*

ISO 14533-2, *Processes, data elements and documents in commerce, industry and administration — Long term signature — Part 2: Profiles for XML Advanced Electronic Signatures (XAdES)*

ISO 22300, *Security and resilience — Vocabulary*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules — Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 9834-1, *Information technology — Procedures for the operation of object identifier registration authorities — Part 1: General procedures and top arcs of the international object identifier tree*

ISO/IEC 9834-8, *Information technology — Procedures for the operation of object identifier registration authorities — Part 8: Generation of universally unique identifiers (UUIDs) and their use in object identifiers*

ISO/IEC 15459-2, *Information technology — Automatic identification and data capture techniques — Unique identification — Part 2: Registration procedures*

ETSI TS 102 853, *Electronic Signatures and Infrastructures (ESI); Signature verification procedures and policies Technical Specification*

ETSI TS 119 612, *Electronic Signatures and Infrastructures (ESI); Trusted Lists*

IETF RFC 3339, *Date and Time on the Internet: Timestamps*

IETF RFC 3986, *Uniform Resource Identifiers*

IETF RFC 4387, *Internet X.509 Public Key Infrastructure, Operational Protocols: Certificate Store Access via HTTP*

IETF RFC 4648:2006, *The Base16, Base32, and Base64 Data Encodings*

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

NIST FIPS 180-4, *Secure Hash Standard (SHS)*

NIST FIPS 186-5, *Digital Signature Standard (DSS)*

PCRE, *Perl Compatible Regular Expressions* [online]. Available at: https://www.pcre.org/

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
machine-readable code
MRC
graphical symbol or electronic device, or a combination of the two, containing a set of signs, characters, patterns or signals 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.

3.2
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* (3.1).

3.3
visible digital seal
VDS
structured data set, often in the form of a *machine-readable code* (3.1), containing a payload and its signature from the issuer

Note 1 to entry: A header identifies the type of payload and the issuer. An optional auxiliary data block may be added after the signature

Note 2 to entry: VDS specified in this document is one of possible various *electronically signed encoded data sets* (3.2).

3.4
asymmetrical cryptography
encryption/decryption operations performed using a key pair: a private key used by the issuer to sign *documents* (3.10) and a public key used to verify the signature

Note 1 to entry: The two keys have an “asymmetric” role, hence the term.

3.5
base36
notation for encoding arbitrary data using a restricted set of symbols made of 36 characters: digits 0 to 9 and letters A to Z

Note 1 to entry: Symbol “Z” has a value of 35

3.6
C40 encoding
encoding to reduce the number of bytes required to encode a string of characters

Note 1 to entry: C40 encoding is explained in ISO/IEC 16022:2006.

3.7
certificate authority
CA
service offered by a *trust service provider* (3.21) to create, issue and produce *certificates* (3.11) on behalf of users, and ensure the integrity of the electronic identification of signatories

Note 1 to entry: The CA signs the certificate (with its own private key) to guarantee the integrity of the certificate and the accuracy of the data contained in the certificates that it issues.

3.8
certificate revocation list
CRL
list of *certificates* (3.11) that have been revoked by the issuing *certificate authority* (3.7)

Note 1 to entry: The CRL shall be in in accordance with IETF RFC 5280.

3.9
digital signature algorithm
DSA
mathematical technique used to validate the authenticity and integrity of a message, software or digital document

Note 1 to entry: These include, but are not limited to, the RSA and ECDSA algorithms defined in NIST FIPS 186-4.

3.10
document
information and the medium on which it is contained

Note 1 to entry: The medium can be paper or any other substrate, magnetic, electronic or optical computer disc, photograph or master sample, or a combination thereof.

3.11
certificate
electronic certificate
X.509 certificate
electronic file attesting that a cryptographic key pair belongs to either a physical or legal person, a hardware component or a software component as identified in the certificate

Note 1 to entry: Certificates are issued by a *certificate authority (CA)* (3.7). By signing the certificate, the CA certifies the association between the key pair with the person, hardware component or software component. A certificate may be revoked if this association can no longer be established. A certificate is valid for a limited amount of time.

3.12
hash
operation that consists of applying a mathematical function to create a digital fingerprint on a data block, transforming the data block into a fixed-size code for authentication and storage purposes

Note 1 to entry: Any change to the original data block results in a change in the hash value.

3.13
manifest
external resource containing information in extensible markup language (XML) format about the *visible digital seal* (3.3) use case, its *schema* (3.18), validation policies and optional extensions

3.14
message pack
binary data exchange format used to represent simple data structures and tables

Note 1 to entry: The purpose of message pack is to be as compact and simple as possible. It is defined in Reference [10].

3.15
online certificate status protocol
OCSP
protocol to validate a *certificate's* (3.11) status, usually to determine if the certificate has been revoked

Note 1 to entry: OCSP is explained in IETF RFC 6960.

Note 2 to entry: OCSP is an alternative to a *certificate revocation list* (3.8).

3.16
regular expression
character string that describes, using a specific syntax, a set of allowed strings or characters

Note 1 to entry: The regular expression shall conform to the Perl Compatible Regular Expressions (PCRE) specification.

3.17
response formatting function
RFF
function specifying how to format and present the output with *visible digital seal* (3.3) verification results

3.18
schema
payload data structure that allows for data encoding, decoding and verification

3.19
symbology
description of numeric, text or binary data encoding in a *machine-readable code* (3.1) defining the redundancy, error correction code mechanisms and specifying the quiet zone around the barcode

3.20
trust service operator
TSO
entity that defines the governance structure and technical requirements of the trust service, and oversees the overall operations

Note 1 to entry: In some industries, the TSO acts as the authentication service body (ASB).

3.21
trust service provider
TSP
entity tasked with defining the *certificate authority (CA)* (3.7) trust framework and governance structure, offering certificate service(s), operating the CA and ensuring compliance with said governance

3.22
trusted entry point
TEP
method provided and/or certified by the *trust service operator* (3.20) having support for the *response formatting function* (3.17), open for additional object identification and authentication systems (OIAS), and able to resolve without ambiguity any unique identifier (UID)

3.23
trust service list
TSL
list containing compliant information about the *trust service operator* (*TSO)* (3.20), the *trust service providers (TSPs)* (3.21) and the TSP's *certificate authority* (3.7) authorized to issue *certificates* (3.11) 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 TSO.

3.24
uniform resource identifier
URI
character string that unambiguously identifies a resource

Note 1 to entry: The syntax shall conform to IETF RFC 3986.

4 General concepts

A VDS is usually represented in the form of one or a combination of MRC(s). It contains data to be protected and the electronic signature of the data by the document issuer. VDSs are read using an optoelectronic or electronic device, e.g. a scanner, 2D barcode reader, RFID reader or a combination of devices.

The detailed implementation of a VDS is always conditioned by a specific use case. Defined by a group of experts, each use case determines the key data fields to be included in the schema, as well as the field constraints. If required, the use case may also include additional verification policies and features defined in TSO extensions to satisfy the business rules for the use case. Use cases are then translated into a machine-readable format (secure XML-format manifest file) so that those who produce and verify the VDSs can interpret and process the information in a standard and deterministic way, while respecting the rules defined for each use case. The manifest is extensible through XML extensions defined by the TSO, with the aim of enabling a richer set of functionalities, such as additional VDS verification policies (e.g. authorized symbologies, signer's legitimacy, validity period), the RFF and post-verification business rules.

Many steps have been taken to minimize the amount of space used by the data carrier and to maximize the amount of space that can be used for data. As such, the VDS does not contain the certificate used for the signature or the definition of the use case; rather, the VDS contains identifiers allowing for their retrieval (see 5.3.2). The VDS payload and signature are also structured to minimize size.

To ensure the reliability of the service, verification of the different elements of the VDS and the chain of trust is essential. Therefore, verification is a normative component to this specification (see Clause 7). Each element supporting the VDS is protected and signed by the TSO to ensure its trustworthiness.

In this document, in order to unambiguously differentiate hexadecimal numbers from others, a prefixed notation “0x” is used.

5 Structures and resources

5.1 General

All URI and endpoints shall be in lower case.

5.2 Trust service list and extensions

5.2.1 General

The TSL shall conform to ETSI TS 119 612, with the exception of the field <SchemeTerritory> which is optional, and include information regarding the TSO and authorized TSP’s certificate authority (CA) to enable trusted service operation.

5.2.2 Extensions

The operation of a VDS trust service requires adding the following three attributes that are not defined in ETSI TS 119 612:

— URI to locate manifests;

— CA reference for each TSP Service;

— URI to locate signing certificates for each CA.

These shall be defined through extensions.

5.2.3 TSO identity

The TSO shall be identified in accordance with ISO/IEC 15459-2 by an Issuing Agency Code (IAC). This IAC code shall be used to locate the TSL.

5.2.4 TSO manifest location

The VDS header includes a reference to the manifest. To locate the manifest, the TSL shall include a URI to the manifest directory.

The manifest directory URI is defined by the extension attribute <VDSManifestResource> in the scheme extensions of the TSL using the following xPath:

```
/TrustServiceStatusList/SchemeInformation/SchemeExtensions/Extension/
vdsext:VDSManifestResource
```

The manifest URI is a concatenation of the manifest directory URI and the manifest ID (in hexadecimal format, always in lower case letters). An example to retrieve manifest 0x89AB01 with the <VDSManifestResource> extension value is as follows:

```
“https://manifest.otentik.codes”:
https://manifest.otentik.codes/89ab01.xml
```

5.2.5 CA reference

The CA reference is a four-character string included in the VDS header to locate the signing certificate and to ensure the CA validity in the TSL. It is composed of:

— CA issuing country (ISO 3166-1 Alpha2), in upper case letters;

— CA identifier: two digits assigned by the TSO.

The CA reference is defined by the extension attribute <VDSAuthorityID> in the TSL's service information extensions using the following xPath:

```
/TrustServiceStatusList/TrustServiceProviderList/TrustServiceProvider/TSPInformation/
ServiceInformationExtensions/Extension/vdsext:VDSAuthorityID
```

5.2.6 Public certificate directory

The VDS header includes a reference to the signing certificate. To locate the certificate, the TSL shall include, for each CA, a URI to the certificate directory. The TSP's CA identifier should be present in the URI.

The certificate endpoint is defined by the attribute <VDSCertResource> in the service information extensions of the TSL using the following syntax:

```
/TrustServiceStatusList/TrustServiceProviderList/TrustServiceProvider/
TSPServices/TSPService/ServiceInformation/ServiceInformationExtensions/Extension/
vdsext:VDSCertResource
```

The certificate URI is a concatenation of the certificate endpoint and the certificate reference number (in base36 format). This URI format shall conform to IETF RFC 4387. An example to retrieve certificate "09HZ" issued by a CA that is assigned the identifier "FR01" and the <VDSCertResource> to "`https://trust.otentik.codes/fr01`" is as follows:

```
https://trust.otentik.codes/fr01/09hz.cer
```


5.2.7 XML security

To ensure its integrity, the TSL shall be electronically signed by the TSO in accordance with ISO 14533-1 CAdES or ISO 14533-2 XAdES-B format. The TSO may detail the required parameters and characteristics of the signature.

5.2.8 Example and verification

See Annex B for a TSL example.

The TSL shall include a xsi:schemaLocation directive to facilitate automated XML validation (see the example in Annex D).

5.3 Manifest

5.3.1 General

The manifest is a machine-readable definition of a use case. It contains various sections: use case information, data schema and optional extensions (defined by the TSO). The VDS header includes a reference to a manifest. The reference number shall be assigned by the TSO.

5.3.2 Information section

This section links the machine-readable manifest identifier to a human-readable use case name and description. The list of attributes and their description is given in Table 1.