NORME INTERNATIONALE

ISO 22376

Première édition
2023-08

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

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

Numéro de référence
ISO 22376:2023(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'ISO attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de propriété revendiqué à cet égard. À la date de publication du présent document, l'ISO n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié tout ou partie de tels droits de brevet.

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/iso/fr/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 292, *Sécurité et résilience*.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

Un cachet électronique visible (CEV) est une représentation d'un ensemble de données structurées, se présentant souvent sous la forme d'un code lisible par machine, utilisé pour garantir l'authenticité et l'intégrité de données clés associées à un document ou à un objet. Le CEV a un coût relativement faible et, grâce à la cryptographie à clé publique, un niveau de sécurité élevé.

Les systèmes basés sur le format du CEV peuvent permettre un suivi et une traçabilité sécurisés, renforcés et interopérables, associés à une authentification anti-contrefaçon.

La fiabilité des données véhiculées par un CEV dépend de la confiance que l'on peut accorder au certificat lié à son environnement cryptographique. Le CEV spécifié dans le présent document est l'une des représentations possibles d'ensembles de données encodées signés électroniquement (ESEDS) comme, par exemple, un identificateur de ressource uniforme (URI) formaté selon la norme GS1 Digital Link et protégé par une signature numérique conforme à l'ISO/IEC 20248. La confiance attendue de ce CEV est fournie par le schéma ESEDS associé.

Le présent document n'interfère pas avec les systèmes d'authentification, de traçabilité et d'identification existants. Il permet de rendre interopérables des environnements techniquement hétérogènes de suivi, de traçabilité et de lutte contre la contrefaçon.

Il est possible de configurer un point d'entrée de confiance (PEC), afin de réduire le nombre d'applications d'identification d'objets en les combinant en un lecteur universel à même de faire face aussi bien aux cas d'utilisation des inspecteurs professionnels que des consommateurs. Le présent document s'adresse aux développeurs et aux utilisateurs qui souhaitent mettre en place des systèmes de suivi, de traçabilité et d'authentification sécurisés et interopérables. Étant donné que la méthode n'est pas liée à une quelconque technologie, elle peut convenir à tous les secteurs industriels où des identifiants uniques (UID) ou des données doivent être sécurisés et inspectés dans un environnement global et multilingue.

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

1 Domaine d'application

Le présent document définit les conditions nécessaires au déploiement interopérable de cachets électroniques visibles (CEV). Il décrit la structure, les formes de représentation possibles ainsi que les processus de production et de vérification des CEV, pour tout type de document ou d'objet auxquels ils se rapportent.

Le présent document ne définit pas d'exigences pour les utilisateurs qui émettent ou vérifient des documents ni pour les utilisateurs qui mettent en œuvre et déploient des CEV.

Le présent document ne s'applique pas aux fonctions de formatage de la réponse (RFF). Ces exigences et fonctions sont définies par un opérateur de service de confiance (OSC) et visent des fonctionnalités telles que les niveaux de sécurité des certificats utilisés et les règles de gouvernance à appliquer aux émetteurs de documents et aux prestataires de services de confiance (PSC) intervenant pendant le processus de production et de lecture des CEV.

Le présent document ne s'applique pas à la gouvernance liée au fonctionnement du schéma CEV. Il n'est pas destiné à remplacer les spécifications des documents de l'Agence nationale des titres sécurisés (ANTS), du Bundesamt für Sicherheit in der Informationstechnik (BSI) et de l'International Civil Aviation Organization (ICAO).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 3166-1, *Codes pour la représentation des noms de pays et de leurs subdivisions — Partie 1: Codes de pays*

ISO 14533-1, *Titre manque — Partie 1: Titre manque*

ISO 14533-2, *Processus, éléments d'informations et documents dans le commerce, l'industrie et l'administration — Signature à long terme — Partie 2: Profils pour les signatures électroniques avancées XML (XAdES)*

ISO 22300, *Sécurité et résilience — Vocabulaire*

ISO/IEC 8825-1, *Technologies de l'information — Règles de codage ASN.1 — Partie 1: Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER)*

ISO/IEC 9834-1, *Technologies de l'information — Procédures opérationnelles pour les organismes d'enregistrement d'identificateur d'objet — Partie 1: Procédures générales et arcs sommitaux de l'arborescence des identificateurs d'objet internationale*

ISO/IEC 9834-8, *Technologies de l'information — Procédures opérationnelles pour les organismes d'enregistrement d'identificateur d'objet — Partie 8: Génération des identificateurs uniques universels (UUID) et utilisation de ces identificateurs dans les composants d'identificateurs d'objets*

ISO/IEC 15459-2, *Technologies de l'information — Identification automatique et techniques de capture de données — Identification unique — Partie 2: Procédures d'enregistrement*

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* [en ligne]. Disponible à l'adresse: https://www.pcre.org/

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO 22300 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

3.1
code lisible par machine
MRC (Machine-Readable Code)
symbole graphique ou dispositif électronique, ou une combinaison des deux, contenant un ensemble de signes, de caractères, de motifs ou de signaux qui peuvent être interprétés par un système d'acquisition

Note 1 à l'article: Les exemples de MRC comprennent, sans s'y limiter, les codes à barres 2D et les étiquettes d'identification par radiofréquence (RFID).

3.2
ensemble de données encodées signé électroniquement
ESEDS (Electronically Signed Encoded Data Set)
ensemble de données structurées contenant l'en-tête, le message, la signature et un bloc de données auxiliaires facultatif

Note 1 à l'article: Le type de données utiles et l'identité de l'émetteur sont inclus dans l'en-tête.

Note 2 à l'article: L'ESEDS peut souvent être exprimé sous forme de *code lisible par machine* (3.1).

3.3
cachet électronique visible
CEV
ensemble de données structurées, souvent sous forme de *code lisible par machine* (3.1), contenant un message et sa signature par l'émetteur

Note 1 à l'article: L'en-tête détermine le type de message et l'émetteur. Un bloc de données auxiliaires facultatif peut être ajouté après la signature.

Note 2 à l'article: Le CEV spécifié dans le présent document est l'un des différents *ensembles de données encodées signés électroniquement* (3.2) possibles.

3.4
cryptographie à clé publique (aussi appelé «cryptographie asymétrique»)
opérations de chiffrement et de déchiffrement exécutées à l'aide d'une paire de clés: une clé privée utilisée par l'émetteur pour signer les *documents* (3.10) et une clé publique servant à vérifier la signature

Note 1 à l'article: Les deux clés ayant un rôle «asymétrique», le terme «cryptographie asymétrique» est utilisé comme synonyme.

3.5
base36
notation pour l'encodage de données arbitraires à l'aide d'un ensemble restreint de symboles composés de 36 caractères: les chiffres 0 à 9 et lettres A à Z

Note 1 à l'article: Le symbole «Z» a la valeur 35.

3.6
encodage C40
encodage réduisant le nombre d'octets requis pour encoder une chaîne de caractères

Note 1 à l'article: L'encodage C40 est expliqué dans l'ISO/IEC 16022:2006.

3.7
autorité de certification
AC
service offert par un *prestataire de services de confiance* (3.21) pour créer, émettre et produire des *certificats* (3.11) au nom des utilisateurs et confirmer l'intégrité de l'identification électronique des signataires

Note 1 à l'article: L'AC signe le certificat (avec sa propre clé privée) pour garantir l'intégrité du certificat et l'exactitude des données contenues dans chaque certificat qu'elle émet.

3.8
liste de révocation des certificats
CRL (Certificate Revocation List)
liste de *certificats* (3.11) qui ont été révoqués par l'*autorité de certification* (3.7) émettrice

Note 1 à l'article: La CRL doit être conforme à l'IETF RFC 5280.

3.9
algorithme de signature numérique
DSA (Digital Signature Algorithm)
technique mathématique utilisée pour valider l'authenticité et l'intégrité d'un message, d'un logiciel ou d'un document numérique

Note 1 à l'article: Les DSA comprennent, sans s'y limiter, les algorithmes RSA et ECDSA définis dans la norme NIST FIPS 186-4.

3.10
document
information et support sur lequel cette information est contenue

Note 1 à l'article: Le support peut être du papier ou un autre type de substrat, un disque électronique ou optique, un support magnétique, une photographie, un échantillon maître ou une combinaison de ces supports.

3.11
certificat
certificat électronique
Certificat X .509
fichier électronique attestant qu'une paire de clés cryptographiques appartient à la personne physique ou morale, ou au composant matériel ou logiciel identifié dans le certificat

Note 1 à l'article: Les certificats sont émis par l'*autorité de certification (AC)* (3.7). En signant un certificat, l'AC certifie l'association entre la paire de clés et la personne ou le composant matériel ou logiciel. Un certificat peut être révoqué si cette relation ne peut plus être établie. Un certificat a une durée de validité déterminée.

3.12
hachage (aussi appelé «condensat»)
application d'une fonction mathématique pour créer une empreinte numérique sur un bloc de données. Ce dernier est ainsi transformé en code de format fixe aux fins d'authentification et de stockage

Note 1 à l'article: Toute modification du bloc de données initial entraîne une modification de la valeur de hachage.

3.13
manifeste
ressource externe contenant des informations au format XML (langage de balisage extensible) sur le cas d'utilisation du *cachet électronique visible* (3.3), son *schéma* (3.18), ses politiques de validation et ses extensions facultatives

3.14
message pack
format d'échange de données binaires utilisé pour représenter des structures de données simples et des tableaux

Note 1 à l'article: Le format message pack se veut le plus simple et compact possible. Il est défini à la Référence [10].

3.15
protocole OCSP
OCSP
protocole de vérification de *certificat* (3.11) en ligne utilisé pour valider l'état d'un certificat, habituellement pour déterminer si le certificat a été révoqué

Note 1 à l'article: Le protocole OCSP est expliqué dans la norme IETF RFC 6960.

Note 2 à l'article: Le protocole OCSP est une solution de remplacement à l'utilisation d'une *liste de révocation des certificats* (3.8).

3.16
expression rationnelle (aussi appelée «expression régulière»)
chaîne de caractères décrivant, à l'aide d'une syntaxe spécifique, un ensemble de chaînes ou de caractères admissibles

Note 1 à l'article: L'expression rationnelle doit être conforme à la spécification PCRE (Perl-Compatible Regular Expression).

3.17
fonction de formatage de la réponse
RFF (Response Formatting Function)
fonction précisant comment formater et présenter les résultats de vérification du *cachet électronique visible* (3.3)

3.18
schéma
structure de données du message permettant l'encodage, le décodage et la vérification des données

3.19
symbologie
décrit l'encodage des données numériques, texte ou binaires dans un *code lisible par machine* (3.1) définissant les mécanismes de redondance et de code de correction d'erreurs et spécifiant la zone blanche autour du code-barres

3.20
opérateur de service de confiance
OSC
entité définissant la structure de gouvernance et les exigences techniques du service de confiance, et qui assure la supervision de l'ensemble des opérations

Note 1 à l'article: Dans certains secteurs d'activité, l'OSC est également l'organisme d'authentification (ASB, *Authentication Service Body*).

3.21
prestataire de services de confiance
PSC
entité ayant la responsabilité de définir le cadre de confiance et la structure de gouvernance de l'*autorité de certification (AC)* (3.7), d'offrir des services de certificats, d'exploiter l'AC et de veiller à la conformité à ladite gouvernance

3.22
point d'entrée de confiance
PEC
méthode fournie et/ou certifiée par l'*opérateur de service de confiance* (3.20) prenant en charge la *fonction de formatage de la réponse* (3.17), ouverte à des systèmes d'identification et d'authentification d'objets (OIAS) supplémentaires, et capable de résoudre sans ambiguïté tout identifiant unique (UID)

3.23
liste des services de confiance
TSL (Trust Service List)
liste contenant des informations conformes sur l'*opérateur de service de confiance (OSC)* (3.20), les *prestataires de services de confiance (PSC)* (3.21) et l'*autorité de certification* (3.7) du PSC autorisée à émettre des *certificats* (3.11) pour signer les *ensembles de données encodées signés électroniquement* (3.2)

Note 1 à l'article: L'ETSI TS 119 612 définit ce qu'est une TSL conforme.

Note 2 à l'article: Les TSL sont extensibles grâce au langage de balisage extensible (XML) défini par l'OSC.

3.24
identificateur de ressource uniforme
URI
chaîne de caractères qui identifie une ressource sans ambiguïté

Note 1 à l'article: La syntaxe doit se conformer à l'IETF RFC 3986.

4 Concepts de base

Un CEV est habituellement représenté sous forme d'un ou de plusieurs MRC. Il contient des données à protéger et la signature électronique de ces données, apposée par l'émetteur du document. Les CEV sont lus à l'aide d'un dispositif électronique ou optoélectronique, par exemple, un scanneur ou un lecteur de codes-barres 2D, un lecteur RFID ou une combinaison de ces dispositifs.

La mise en œuvre détaillée d'un CEV donné est toujours régie par un cas d'utilisation spécifique. Défini par un groupe d'experts, chaque cas d'utilisation détermine les champs de données clés devant être inclus dans le schéma, ainsi que les contraintes de chaque champ. Au besoin, le cas d'utilisation peut inclure des politiques de vérification supplémentaires et des fonctionnalités définies dans les extensions de l'OSC afin de respecter les règles d'affaires du cas d'utilisation. Le cas d'utilisation est ensuite traduit en format lisible par machine (fichier manifeste en format XML sécurisé) afin que le CEV puisse être interprété et traité de manière normalisée et déterministe par la personne morale ou physique qui l'a produit et par celles devant le vérifier, conformément aux règles prescrites dans chaque cas d'utilisation. Le manifeste peut être étendu à l'aide d'extensions XML définies par l'OSC dans le but de permettre un plus grand ensemble de fonctionnalités, telles que des politiques de vérification de CEV supplémentaires (par exemple, symbologies autorisées, légitimité des signataires, période de validité), l'utilisation d'une RFF et des règles d'affaires post-vérification.

De nombreuses actions ont été mises en place pour réduire au minimum l'espace utilisé par le support de données et maximiser l'espace utilisable par les données. Ainsi, le CEV ne contient pas le certificat utilisé pour la signature ni la définition du cas d'utilisation; il contient, en revanche, des identifiants qui permettent d'accéder à ces éléments (voir 5.3.2). De plus, le message et la signature du CEV sont structurés de manière à ce que leur taille soit réduite.

Pour assurer la fiabilité du service, la vérification des différents éléments du CEV et de la chaîne de confiance est essentielle. Ainsi, la vérification est un composant normatif de cette spécification technique (voir Article 7). Chaque élément requis par le CEV est protégé et signé par l'OSC pour en assurer la fiabilité.

Afin de différencier sans ambiguïté les nombres hexadécimaux des autres nombres, la notation préfixée «0x» est utilisée dans le présent document.

5 Structures et ressources

5.1 Généralités

Tous les URI et points d'accès doivent être en minuscules.

5.2 Liste des services de confiance et extensions

5.2.1 Généralités

La TSL doit être conforme à l'ETSI TS 119 612, à l'exception du champ <SchemeTerritory> qui est facultatif. La TSL doit inclure les informations relatives à l'OSC et à l'autorité de certification (AC) du PSC autorisé afin de permettre l'exploitation des services de confiance.

5.2.2 Extensions

L'exploitation d'un service de confiance d'un CEV exige l'ajout des trois attributs suivants non définis dans l'ETSI TS 119 612:

— une adresse URI pour localiser les manifestes;

— une référence d'AC pour chaque service d'un PSC;

— une adresse URI pour localiser les certificats de signature de chaque AC.

Ces attributs doivent être définis par des extensions.

5.2.3 Identité d'un OSC

L'OSC doit être identifié conformément à l'ISO/IEC 15459-2 par le code de l'agence émettrice (IAC, *Issuing Agency Code*). Ce code IAC doit être utilisé pour localiser la TSL.

5.2.4 Emplacement du manifeste d'un OSC

L'en-tête du CEV comprend une référence au manifeste. Pour qu'il soit possible de localiser le manifeste, la TSL doit comprendre une adresse URI pointant vers le répertoire de manifestes.

L'URI du répertoire de manifestes est définie par l'attribut d'extension <VDSManifestResource> dans les extensions de schéma de la TSL utilisant le XPath suivant:

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

L'URI du manifeste est une concaténation de l'URI du répertoire des manifestes et de l'ID du manifeste (au format hexadécimal, toujours en lettres minuscules). Voici un exemple permettant de récupérer le manifeste 0x89AB01 avec la valeur d'extension <VDSManifestResource>:

```
"https://manifest.otentik.codes":
https://manifest.otentik.codes/89ab01.xml
```

5.2.5 Référence de l'AC

La référence de l'AC est une chaîne de quatre caractères faisant partie de l'en-tête du CEV et permettant de localiser le certificat de signature et d'assurer la validité de l'AC dans la TSL. Elle est composée des éléments suivants:

— pays émetteur de l'AC (ISO 3166-1 Alpha2), en lettres majuscules;

— identifiant de l'AC: deux chiffres attribués par l'OSC.

La référence de l'AC est définie par l'attribut d'extension <VDSAuthorityID> dans les extensions d'information sur le service <ServiceInformationExtensions> de la TSL utilisant le XPath suivant:

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


5.2.6 Répertoire des certificats publics

L'en-tête du CEV comprend une référence au certificat de signature. Pour qu'il soit possible de localiser le certificat, la TSL doit comprendre une adresse URI vers le répertoire de certificats propre à chaque AC. Il convient que l'identifiant d'AC du PSC soit présent dans l'URI.

Le point d'accès du certificat est défini par l'attribut <VDSCertResource> dans les extensions d'information sur le service <ServiceInformationExtensions> de la TSL utilisant la syntaxe suivante:

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

L'URI du certificat est une concaténation du point d'accès du certificat et du numéro de référence du certificat (en format Base36). Le format de l'URI doit se conformer à l'IETF RFC 4387. Voici un exemple permettant d'extraire le certificat «09HZ» émis par l'AC à qui il a été attribué l'identifiant «FR01» et l'attribut <VDSCertResource> sous "`https://trust.otentik.codes/fr01`":

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

5.2.7 Sécurité XML

Pour que son intégrité soit garantie, la TSL doit être signée électroniquement par l'OSC au format CAdES conformément à l'ISO 14533-1 ou au format XAdES-B conformément à l'ISO 14533-2. L'OSC peut détailler les paramètres et caractéristiques requis de la signature.