NORME INTERNATIONALE

ISO 16678

Première édition
2014-07-01

Lignes directrices pour l'identification interopérable d'objets et systèmes d'authentification associés destinés à décourager la contrefaçon et le commerce illicite

Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

Numéro de référence
ISO 16678:2014(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
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 (CEI) 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/CEI, 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/CEI, Partie 2 (voir www.iso.org/directives).

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

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 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'OMC concernant les obstacles techniques au commerce (OTC), voir le lien suivant: Avant-propos — Informations supplémentaires.

Le Comité chargé de l'élaboration du présent document est l'ISO/TC 247, *Mesures de prévention et de contrôle de la fraude.*

Introduction

La présente Norme internationale pose trois hypothèses fondamentales. Premièrement: la détection des objets de contrefaçon est une tâche complexe et souvent difficile. Deuxièmement: l'information pertinente sur l'identité de l'objet considéré simplifie le processus de détection des contrefaçons. Et troisièmement: l'information pertinente est souvent complexe et dure à trouver.

Le principal objectif de la présente Norme internationale est de simplifier l'accès et la diffusion d'informations d'identification pertinentes à des agents de confiance (contrôleurs) dans le cadre du processus d'authentification d'objets.

Pour atteindre cet objectif, le document fournit des lignes directrices destinées à faciliter l'accès et l'utilisation des informations sur l'identité des objets. Les données et informations d'identification peuvent se trouver en différents endroits, notamment dans les systèmes de vérification et d'authentification. Permettre aux contrôleurs d'accéder aux informations d'identification les aide à détecter les contrefaçons. Aider les contrôleurs à trouver les informations d'identification les aide à détecter les contrefaçons. Ces observations nous amènent aux conclusions suivantes:

> L'amélioration de l'interopérabilité des systèmes d'identification d'objets et des systèmes d'authentification associés devrait rendre l'utilisation de ces systèmes plus faciles pour les contrôleurs. L'amélioration de la facilité d'utilisation devrait accroître l'utilisation par les contrôleurs de la multitude de systèmes contenant de l'information pertinente, augmentant ainsi la détection des contrefaçons et réduisant les pertes dues à la contrefaçon.

La présente Norme internationale se concentre sur l'acheminement des demandes d'informations sur des objets à un service autorisé approprié, puis sur l'acheminement des réponses aux contrôleurs.

Les systèmes d'identification d'objets utilisent généralement des identificateurs uniques (UID) pour faire référence ou accéder aux informations relatives aux objets. Un UID peut être assigné à une classe d'objets ou à un objet distinct. Dans les deux cas, l'UID peut améliorer la détection des contrefaçons et des fraudes, bien que les UID assignés à des instances individuelles puissent être plus efficaces. La présente Norme internationale est organisée en six (6) grandes parties:

— **Domaine d'application:** Déclare que la présente Norme internationale se limite à fournir uniquement des lignes directrices et des conseils. La présente Norme internationale ne contient aucune exigence.

— **Termes:** Donne la signification contextuelle des termes importants utilisés dans la présente Norme internationale, tels que «agent de confiance», «contrôleur» et «interopérabilité sémantique».

— **Vue d'ensemble:** Aperçu de la façon dont les informations relatives aux objets sont utilisées pour détecter les contrefaçons.

— **Principes essentiels:** Concepts et valeurs qui ont influencé les lignes directrices.

— **Lignes directrices:** Recommandations censées améliorer l'interopérabilité des systèmes capables de fournir aux contrôleurs des informations sur les objets.

— **Annexes informatives:** Exemples spécifiques illustrant certains des concepts présentés dans la présente Norme internationale**.**

Résultats souhaités

Plus les solutions de validation ou d'authentification sont utilisées, plus elles deviennent efficaces dans la détection et la prévention des fraudes telles que la contrefaçon et le détournement illégal. La présente Norme internationale vise à permettre une identification fiable et sûre des objets afin de décourager l'introduction d'objets illégaux sur le marché.

L'un des objectifs de la présente Norme internationale est de décrire un cadre dans lequel les diverses solutions d'identification des objets sont interopérables et la confiance accrue, et donc d'accroître leur

utilisation. Le cadre doit également comprendre des solutions permettant simplement de détecter certaines contrefaçons sans procéder à l'authentification des produits. De même, le cadre doit également comprendre une solution permettant d'évaluer un élément d'authentification uniquement.

Étant donné que l'on s'attend également à ce que les systèmes d'identification d'objets eux-mêmes soient contrefaits et copiés, la présente Norme internationale établit une méthode permettant de prouver formellement qu'une description à distance d'un objet peut être digne de confiance. Une attention particulière est portée à la prévention des interférences entre différentes implémentations indépendantes de ces systèmes ainsi qu'à l'affectation d'une référence d'identification unique et non ambiguë servant à de multiples usages et applications.

Le principe de base de la conception du système est qu'un manque de confiance et d'interopérabilité provoque une «réticence» de la part des utilisateurs. En réduisant cette réticence, il est possible d'accroître la sensibilisation et l'utilisation, et donc la détection et la dissuasion de la fraude.

Lignes directrices pour l'identification interopérable d'objets et systèmes d'authentification associés destinés à décourager la contrefaçon et le commerce illicite

1 Domaine d'application

La présente Norme internationale décrit le cadre relatif aux systèmes d'identification et d'authentification. Elle fournit des recommandations et des lignes directrices de bonne pratique concernant les points suivants:

— conséquences et lignes directrices relatives à:

  — la gestion et la vérification des identificateurs; et

  — l'expression physique des identificateurs;

  — la diligence raisonnable des participants;

— filtrage de tous les participants intégrés au système;

— relation entre l'identificateur unique et les éventuels éléments d'authentification qui lui sont associés;

— questions relatives à l'identification du contrôleur et à tout accès autorisé à des informations protégées concernant l'objet; et

— historique (journaux) d'accès des contrôleurs.

En conséquence, la présente Norme internationale établit un cadre et décrit les unités fonctionnelles utilisées pour obtenir la fiabilité et l'interopérabilité de ces systèmes.

La présente Norme internationale ne spécifie pas de solutions techniques spécifiques, mais décrit les processus, les fonctions et les unités fonctionnelles en utilisant un modèle générique pour illustrer ce que les différentes solutions ont en commun.

Les systèmes d'identification des objets peuvent incorporer d'autres fonctions et caractéristiques telles que la traçabilité de la chaîne d'approvisionnement, la traçabilité de la qualité, les activités de commercialisation et autres, mais ces aspects ne relèvent pas du domaine d'application des présentes lignes directrices.

NOTE La présente Norme internationale ne se réfère pas à des exigences industrielles spécifiques telles que les codes d'articles internationaux (EAN).

2 Termes, définitions, symboles et acronymes

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

2.1 Termes et définitions

2.1.1
système de gestion des données d'attributs
ADMS
système qui mémorise, gère et contrôle l'accès aux données concernant des objets

2.1.2
authentification
processus de corroboration d'une entité ou d'attributs avec un niveau d'assurance spécifié ou entendu

[SOURCE: ISO/CEI 29115]

2.1.3
fonction d'authentification
fonction réalisant l'authentification

2.1.4
source autorisée
origine officielle d'un attribut qui est également responsable de la mise à jour de cet attribut

2.1.5
copie du dépositaire
copie qui est subordonnée à la source autorisée

2.1.6
entité
quelque chose ayant une existence séparée et distincte et qui peut être identifiée dans un contexte

Note 1 à l'article: Une entité peut être une personne, une organisation, un objet physique, une classe d'objets ou un objet virtuel.

[SOURCE: ISO/CEI 29115]

2.1.7
identification
processus de reconnaissance des attributs qui identifient l'objet

[SOURCE: ISO/CEI 29115]

2.1.8
identificateur
ensemble spécifié d'attributs assignés à une entité à des fins d'identification

2.1.9
identité
ensemble d'attributs liés à une entité

Note 1 à l'article: Une identité peut avoir des attributs uniques permettant de distinguer un objet de tous les autres.

Note 2 à l'article: L'identité peut être considérée en termes de personne, d'organisation et d'objets (physiques et virtuels).

2.1.10
contrôleur
toute personne qui utilise la fonction d'examen de l'objet (OEF) dans le but d'évaluer un objet

Note 1 à l'article: Tout participant à ce système peut agir comme un contrôleur.

Note 2 à l'article: Les contrôleurs peuvent avoir différents niveaux de qualification et de formation.

Note 3 à l'article: Le contrôleur peut être un système automatique.

2.1.11
historique d'accès d'un contrôleur
journaux d'accès indiquant de façon détaillée quand les codes d'identification uniques (UID) ont été contrôlés, éventuellement par quel contrôleur (privilégié) et éventuellement depuis quel emplacement spécifique

Note 1 à l'article: Les horodatages sont souvent utilisés.

2.1.12
interopérabilité
aptitude d'un point d'entrée unique à acheminer les demandes relatives à des objets portant un UID jusqu'à la source responsable autorisée en vue d'une fonction de vérification de confiance (TVF)

Note 1 à l'article: Aptitude de multiples systèmes d'authentification à fournir des réponses similaires à des groupes d'utilisateurs.

2.1.13
objet
toute entité unique et distincte pouvant être identifiée

2.1.14
fonction d'examen de l'objet
OEF
processus de recherche ou de détermination de l'UID ou autre attribut destiné à l'authentification

Note 1 à l'article: D'autres attributs peuvent aider à l'évaluation de l'UID dans ce processus.

2.1.15
propriétaire
entité qui contrôle légalement les droits de licence et d'utilisateur et la diffusion de l'objet associé à l'UID

2.1.16
participant
fournisseurs de solutions, pour les systèmes interopérables d'identification d'objets et d'authentification associés et leurs groupes d'utilisateurs comprenant, sans toutefois s'y limiter, les détenteurs de droits, les agents des douanes, les distributeurs et les consommateurs

2.1.17
interopérabilité sémantique
aptitude de deux (ou plus) systèmes ou services à interpréter et utiliser automatiquement des informations échangées avec exactitude

2.1.18
interopérabilité syntactique
aptitude de deux (ou plus) systèmes ou services à échanger des informations structurées

2.1.19
fonction de traitement des interrogations de confiance
TQPF
fonction fournissant une passerelle vers la fonction de vérification de confiance (TVF) et le système de gestion des données d'attributs (ADMS)

Note 1 à l'article: Elle inclut un logiciel fonctionnant localement sur un outil portable.

2.1.20
fonction de vérification de confiance
TVF
fonction qui vérifie si un UID reçu est valide ou non et qui gère la réponse selon des règles et des droits d'accès

2.1.21
identificateur unique
UID
code qui représente un ensemble unique et spécifique d'attributs liés à un objet ou à une classe d'objets pendant toute sa vie dans un domaine et un périmètre particuliers d'un système d'identification d'objets

2.1.22
vérification
contrôle visant à s'assurer qu'un UID existe et qu'il est valide dans un système d'identification d'objets

Note 1 à l'article: La vérification peut détecter certains types de fraude, mais ne prouve pas par elle-même qu'une entité est authentique.

2.2 Abréviations et acronymes

ADMS système de gestion des données d'attributs

AI identificateur d'application (voir MH10.8.2) (ang. : Application Identifier)

CA autorité de certification (ang. : Certification Authority)

DI identificateur de données (voir MH10.8.2) (ang. : Data Identifier)

OEF fonction d'examen d'objet (ang. : Object Examination Function)

RFF fonction de formatage de la réponse (ang. : Response Formatting Function)

TQPF fonction de traitement des interrogations de confiance (ang. : Trusted Query Processing Function)

TVF fonction de vérification de confiance (ang. : Trusted Verification Function)

UID identificateur unique (ang. : Unique Identifier)

3 Vue d'ensemble

3.1 Généralités

L'interopérabilité de ces systèmes offre l'avantage d'améliorer la détection des contrefaçons et des fraudes par:

— une utilisation croissante par des groupes d'utilisateurs spécifiques,

— une augmentation du nombre d'objets contrôlés,

— un accès croissant aux sources autorisées, et

— une réduction des coûts:

  — formation;

  — équipement;

  — développement;

  — déploiement;

  — durée d'inspection.

Une fois que l'interopérabilité est établie et que ces systèmes sont largement déployés, un contrôleur utilise un identificateur pour obtenir des renseignements sur un objet qui l'aideront à prendre des dispositions concernant cet objet. Le contrôleur disposerait d'une preuve crédible que les informations fournies en réponse à l'interrogation sont exactes et fiables.

Il est conseillé à tous les participants de remplir leurs rôles avec la diligence requise.

— Il convient d'envisager un audit et une validation des prestataires de services pour s'assurer qu'ils agissent de bonne foi et ne sont pas des agents de menace opérant derrière une «façade» trompeuse.

— Il convient d'envisager un audit et une validation des fabricants pour s'assurer qu'ils respectent des processus documentés et entrent des informations exactes dans les systèmes.

— Il convient que les parties intéressées qui ont besoin d'être informées obtiennent l'accréditation appropriée pour procéder à des interrogations de telle sorte que le détenteur des droits puisse diffuser les informations de manière socialement responsable.

3.2 Systèmes d'identification d'objets (en service)

3.2.1 Généralités

Les systèmes d'identification d'objets sont généralement constitués d'unités fonctionnelles telles que décrites dans le modèle (Figure 1) ci-dessous.

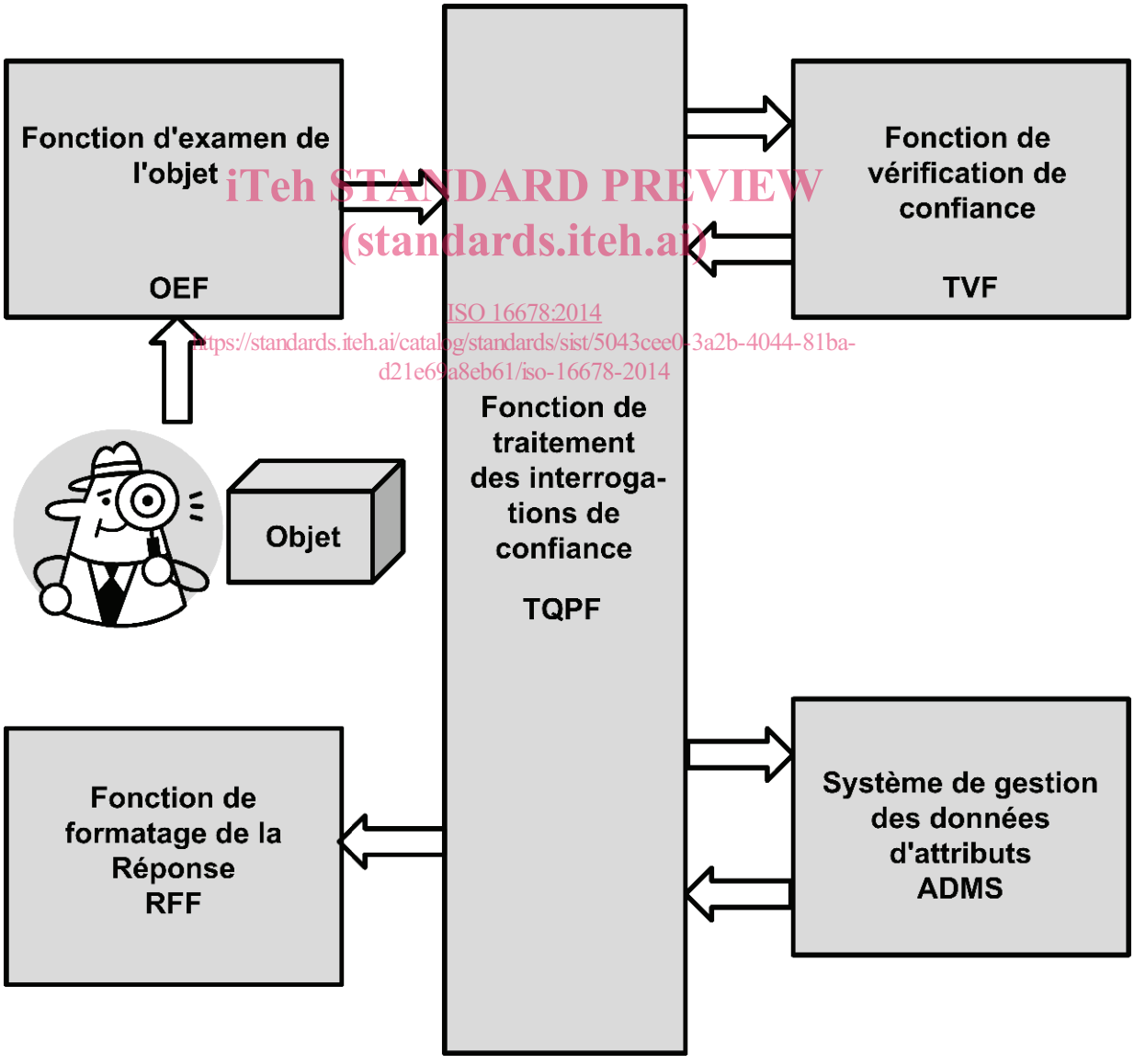

Figure 1 — Modèle de contrôle d'un objet

Le modèle ne fait aucune hypothèse quant à la façon dont les fonctions sont implémentées. Plusieurs instances d'une fonction peuvent exister dans le système. Différentes fonctions peuvent être combinées dans un seul service.

À titre d'illustration, des exemples d'implémentation de ce modèle sont donnés à l'Annexe C.

3.2.2 Fonction d'examen d'objet (OEF)

Le contrôleur examine un objet d'intérêt (tel qu'un bien matériel) afin de déterminer si l'objet possède un UID. Lorsqu'un UID est trouvé, un examen complémentaire peut être nécessaire pour déterminer le(s) service(s) de traitement des interrogations de confiance de fonction susceptible(s) de connaître cet UID. La fonction formule une interrogation qui peut être constituée uniquement d'un UID, d'une combinaison de l'UID et de données liées à l'accréditation du contrôleur ou d'autres données d'attributs physiques comprenant des éléments d'authentification intrinsèques pouvant identifier de façon unique un objet, par exemple une image numérique. La fonction d'examen d'objet se termine lorsqu'une interrogation est soumise à une ou plusieurs TQPF. Lorsque le processus est répété de manière itérative, l'OEF peut évaluer la réponse concernant l'interrogation précédente.

3.2.3 Fonction de traitement des interrogations de confiance

Une TQPF achemine les informations entre les autres fonctions selon des règles définies. La TQPF peut examiner l'authentifiant des parties demandeuses selon des règles définies. La TQPF peut être répartie entre plusieurs services.

Par exemple, une TQPF peut acheminer une interrogation formée par un OEF vers la TVF appropriée ou une TQPF peut combiner la réponse de vérification ou d'authentification d'une TVF à l'authentifiant d'un contrôleur pour former une interrogation dans un ADMS.

3.2.4 Fonction de vérification de confiance

La TVF vérifie si l'UID existe dans le domaine. Il convient que la TVF vérifie l'accréditation de la TQPF demandeuse. Il convient que la TVF applique les droits d'accès en se fondant sur des règles définies. Elle peut répondre à la source de l'interrogation ou par l'intermédiaire d'une ou plusieurs autres TQPF. La réponse contient généralement des informations de vérification concernant l'UID (l'UID est-il valide ou non ?). La TVF peut également générer des alertes pour les parties intéressées. Il convient que la TVF protège les données sensibles contre tout accès non autorisé.

La TVF peut exécuter une procédure ou un algorithme d'authentification sur les informations (données) reçues.

3.2.5 Système de gestion des données d'attributs

Un ADMS est la source autorisée de données de référence concernant les objets. Il convient qu'un seul enregistrement de données de référence soit associé à chaque attribut d'objet. Lorsque plusieurs instances d'enregistrements de données d'attribut existent, il convient qu'un seul d'entre eux soit l'enregistrement «principal» et tous les autres des enregistrements «subordonnés». Différents attributs d'un objet peuvent résider dans différentes bases de données. De multiples bases de données peuvent exister dans un environnement fédéré.

Un ADMS reçoit une réponse (via une TQPF) d'une TVF. L'ADMS vérifie les autorisations de la TQPF demandeuse et du contrôleur. Il convient que les droits d'accès soient basés sur des autorisations et des règles. L'ADMS répond avec des données sélectionnées correspondant à la demande et filtrées par des règles. La réponse peut résoudre toutes les questions du contrôleur ou peut inclure des informations sur la façon de procéder. Lorsqu'une réponse contient des instructions supplémentaires, un contrôleur décide de la nécessité d'une action supplémentaire en lançant une nouvelle interrogation.

Dans un ADMS, les attributs peuvent contenir des informations détaillées sur la façon d'authentifier des objets ou de procéder à un examen complémentaire.

