NORME INTERNATIONALE

ISO/IEC 15408-1

Troisième édition
2009-12-15

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 1: Introduction et modèle général

Information technology — Security techniques — Evaluation criteria for IT security —
Part 1: Introduction and general model

Numéro de référence
ISO/IEC 15408-1:2009(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +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) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organismes internationaux, gouvernementaux et non gouvernementaux, en liaison avec l'ISO et le IEC participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est attirée 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 et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/IEC 15408-1 a été élaborée par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*. Le texte identique de l'ISO/IEC 15408 est publié par les organisations commanditaires du projet Critères communs sous le titre Common Criteria for Information Technology Security Evaluation (Critères Communs pour l'évaluation de la sécurité des technologies de l'information). La source XML commune aux deux publications peut être obtenue à l'adresse http://www.commoncriteriaportal.org/cc/.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 15408-1:2005), qui a fait l'objet d'une révision technique.

L'ISO/IEC 15408 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI:*

— *Partie 1: Introduction et modèle général*;

— *Partie 2: Composants fonctionnels de sécurité*;

— *Partie 3: Exigences d'assurance de sécurité*.

La présente version corrigée de l'ISO/IEC 15408-1:2009 incorpore diverses corrections éditoriales portant sur:

— la terminologie: correction des termes «problème de sécurité» et «domaines de sécurité»;

— le paragraphe 8.3: explication de la notion de conformité stricte et suppression de l'ancienne Figure 4.

Introduction

L'ISO/IEC 15408 autorise une comparabilité entre les résultats d'évaluations de sécurité indépendantes. À cet effet, l'ISO/IEC 15408 propose un ensemble commun d'exigences applicables aux fonctionnalités de sécurité des produits de technologies de l'information (TI) et aux mesures d'assurance appliquées à ces produits TI au cours d'une évaluation de sécurité. Ces produits TI peuvent être mis en œuvre dans du matériel, des microprogrammes ou des logiciels.

Le processus d'évaluation établit un niveau de confiance quant à la capacité des fonctionnalités de sécurité de ces produits TI et des mesures d'assurance qui leur sont appliquées à satisfaire à ces exigences. Les résultats d'évaluation peuvent aider les consommateurs à déterminer si ces produits TI répondent à leurs besoins de sécurité.

L'ISO/IEC 15408 constitue un guide utile pour le développement, l'évaluation et/ou l'acquisition de produits TI dotés de fonctionnalités de sécurité.

L'ISO/IEC 15408 est volontairement souple pour permettre d'appliquer diverses méthodes d'évaluation à différentes propriétés de sécurité d'une vaste gamme de produits TI. Il est par conséquent recommandé aux utilisateurs de la présente norme de prendre toutes les précautions nécessaires pour éviter d'utiliser une telle flexibilité à mauvais escient. Par exemple, l'utilisation de l'ISO/IEC 15408 combinée à des méthodes d'évaluation inappropriées, à des propriétés de sécurité inadaptées ou à des produits TI incompatibles peut conduire à des résultats d'évaluation dénués de sens.

Ainsi, le fait qu'un produit TI ait été évalué n'a de sens que dans le contexte des propriétés de sécurité qui ont été effectivement évaluées et des méthodes d'évaluation qui ont été employées. Il est recommandé aux autorités d'évaluation de vérifier soigneusement les produits, propriétés et méthodes afin de déterminer si une évaluation produira des résultats pertinents. Par ailleurs, les acheteurs de produits évalués sont invités à tenir compte scrupuleusement de ce contexte pour déterminer si le produit évalué est utile et s'il s'applique à leur situation et à leurs besoins spécifiques.

L'ISO/IEC 15408 traite de la protection des biens sensibles contre toute divulgation, modification ou perte d'usage non autorisée. Les catégories de protection relatives à ces trois types de faille de sécurité sont communément désignées par les termes de confidentialité, d'intégrité et de disponibilité, respectivement. L'ISO/IEC 15408 peut également s'appliquer à des aspects de la sécurité TI ne relevant pas de ces trois catégories. L'ISO/IEC 15408 s'applique aux risques liés à des activités humaines (malveillantes ou autres) ainsi qu'aux risques qui ne relèvent pas des activités humaines. Au-delà de la sécurité TI, l'ISO/IEC 15408 peut être appliquée dans d'autres aspects des technologies de l'information, bien qu'elle ne revendique aucune applicabilité dans ces domaines.

Il est établi que certains sujets n'entrent pas dans le domaine d'application de l'ISO/IEC 15408 parce qu'ils impliquent des techniques spécialisées ou parce qu'ils relèvent dans une certaine mesure d'aspects annexes à la sécurité TI. Certains d'entre eux sont identifiés ci-dessous.

a) L'ISO/IEC 15408 ne contient aucun critère d'évaluation de la sécurité relevant de mesures de sécurité administratives qui ne sont pas directement liées à des fonctionnalités de sécurité TI. Il est cependant établi que l'utilisation ou l'appui de mesures administratives, telles que des contrôles organisationnels ou physiques, l'intervention de personnel ou l'application de procédures, peut souvent contribuer à obtenir une sécurité significative.

b) L'évaluation de certains aspects physiques techniques de la sécurité TI, tels que le contrôle des émanations électromagnétiques, n'est pas spécifiquement couverte, bien que de nombreux concepts abordés dans le présent document s'appliquent à ce domaine.

c) L'ISO/IEC 15408 ne couvre pas la méthodologie d'évaluation qu'il convient d'utiliser pour appliquer les critères. Cette méthodologie est décrite dans l'ISO/IEC 18045.

d) De même, l'ISO/IEC 15408 ne traite pas du cadre administratif et juridique dans lequel les autorités d'évaluation peuvent appliquer ces critères. Il est cependant prévu que l'ISO/ 15408 soit utilisée à des fins d'évaluation dans le contexte d'un tel cadre.

e) Les procédures d'utilisation des résultats d'évaluation dans le cadre d'une accréditation ne relèvent pas du domaine d'application de l'ISO/IEC 15408. Une accréditation désigne le processus administratif consistant à accorder l'autorisation d'exploiter un produit TI (ou un ensemble de tels produits) dans son environnement opérationnel, y compris pour l'ensemble de ses composants ne relevant pas des technologies de l'information. Les résultats du processus d'évaluation servent de données d'entrée au processus d'accréditation. Cependant, puisque d'autres techniques se révèlent plus adaptées pour l'appréciation des propriétés qui ne relèvent pas des technologies de l'information ainsi que de leur relation avec les composants de sécurité TI, il convient que les organismes d'accréditation formulent des dispositions distinctes pour traiter de ces aspects.

f) Le sujet des critères pour l'appréciation des qualités inhérentes des algorithmes cryptographiques n'est pas abordé dans l'ISO/IEC 15408. Dans l'éventualité où une appréciation indépendante des propriétés mathématiques de cryptographie serait nécessaire, le schéma d'évaluation en vertu duquel est appliquée l'ISO/IEC 15408 doit prévoir des dispositions à cet égard.

La terminologie ISO, telle que «peut/peuvent», «informative», «normative», «doit/doivent» ou «il convient de/que», telle qu'elle est utilisée dans le présent document, est définie dans les Directives ISO/IEC, Partie 2. Noter que le terme «il convient» possède un sens supplémentaire qui s'applique dans le cadre de l'utilisation de la présente norme. Voir la note ci-dessous. La définition suivante est donnée pour l'utilisation de la locution «il convient» dans l'ISO/IEC 15408.

il convient

Dans un texte normatif, «il convient» est utilisé pour indiquer «qu'entre plusieurs possibilités, l'une est recommandée car particulièrement appropriée, sans mentionner ni exclure les autres, ou qu'une certaine manière de faire est préférée sans être nécessairement exigée.» (Directives ISO/IEC, Partie 2).

NOTE Dans l'ISO/IEC 15408, «sans être nécessairement exigée» est interprété dans le sens où le choix d'une autre possibilité exige de justifier la raison pour laquelle l'option préférée n'a pas été retenue.

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 1: **Introduction et modèle général**

1 Domaine d'application

La présente partie de l'ISO/IEC 15408 établit les concepts et principes généraux de l'évaluation de la sécurité des technologies de l'information (TI). Elle spécifie le modèle général d'évaluation donné par les différentes parties de la norme qui, dans son intégralité, est destinée à servir de base à l'évaluation des propriétés de sécurité des produits TI.

La Partie 1 fournit une vue d'ensemble de toutes les parties de la norme ISO/IEC 15408. Elle décrit les différentes parties de la norme, définit les termes et abréviations à utiliser dans toutes les parties de la norme, établit le concept fondamental d'une cible d'évaluation (TOE, de l'anglais *Target of Evaluation*), spécifie le contexte d'une évaluation et décrit le public à qui s'adressent les critères d'évaluation. Elle fournit en outre une introduction aux concepts de sécurité de base nécessaires pour l'évaluation de produits TI.

Elle définit les diverses opérations dans le cadre desquelles les composants fonctionnels et d'assurance décrits dans l'ISO/IEC 15408-2 et dans l'ISO/IEC 15408-3 peuvent être adaptés par l'utilisation d'opérations autorisées.

Elle spécifie les concepts clés de profils de protection (PP), les ensembles d'exigences de sécurité et le sujet de la conformité, et décrit les conséquences d'une évaluation ainsi que les résultats d'une évaluation. La présente partie de l'ISO/IEC 15408 donne des lignes directrices pour la spécification de cibles de sécurité (ST, de l'anglais *Security Targets*) et fournit une description de l'organisation des composants sur l'ensemble du modèle. Des informations générales sur la méthodologie d'évaluation sont données dans l'ISO/IEC 18045 et le domaine d'application des plans d'évaluation est fourni.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application de l'ISO/IEC 15408, Partie 1. 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/IEC 15408-2, *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 2: Composants fonctionnels de sécurité*

ISO/IEC 15408-3, *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 3: Composants d'assurance de sécurité*

ISO/IEC 18045, *Technologies de l'information — Techniques de sécurité — Méthodologie pour l'évaluation de sécurité TI*

3 Termes et définitions

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

NOTE Le présent article contient uniquement les termes qui sont employés dans un sens spécifique dans l'ensemble des normes ISO/IEC 15408. Certaines combinaisons de termes communs utilisées dans l'ISO/IEC 15408, bien qu'elles ne méritent pas de figurer dans le présent article, sont explicitées pour des raisons de clarté étant donné le contexte dans lequel elles sont utilisées.

3.1 Termes et définitions communs à l'ISO/IEC 15408

3.1.1
actions indésirables
actions exécutées par un agent menaçant sur un bien sensible

3.1.2
biens sensibles
entités auxquelles le propriétaire de la TOE accorde vraisemblablement de la valeur

3.1.3
affectation
spécification d'un paramètre identifié dans un composant (de l'ISO/IEC 15408) ou une exigence

3.1.4
assurance
fondements de la confiance dans le fait qu'une TOE satisfait à ses SFR

3.1.5
potentiel d'attaque
mesure de l'effort à déployer lors de l'attaque d'une TOE, exprimée en termes d'expertise, de ressources et de motivation d'un attaquant

3.1.6
augmentation
ajout d'une ou de plusieurs exigences à un paquet

3.1.7
données d'authentification
informations utilisées pour vérifier l'identité annoncée d'un utilisateur

3.1.8
utilisateur autorisé
utilisateur d'une TOE qui a le droit d'effectuer une opération, en accord avec les SFR

3.1.9
classe
groupement de familles ISO/IEC 15408 qui partagent un thème commun

3.1.10
compréhensible
ordonné de manière logique et ayant un sens perceptible

Note 1 à l'article: à l'article Pour la documentation, cela couvre à la fois le texte réel et la structure du document, en des termes qui soient compréhensibles pour le public cible.

3.1.11
complet
propriété confirmant que toutes les parties nécessaires d'une entité ont été fournies

Note 1 à l'article: à l'article Sur le plan de la documentation, cela signifie que toutes les informations pertinentes sont traitées dans la documentation, avec un niveau de détail tel qu'elles ne nécessitent aucune explication supplémentaire à ce niveau d'abstraction.

3.1.12
composant
le plus petit ensemble sélectionnable d'éléments sur lequel des exigences peuvent être fondées

3.1.13
paquet d'assurance composé
paquet d'assurance constitué des exigences dérivées de l'ISO/IEC 15408-3 (essentiellement de la classe ACO), représentant un point sur une échelle d'assurance de composition prédéfinie par l'ISO/IEC 15408

3.1.14
confirmer
déclarer que quelque chose a été examiné en détail avec un niveau de suffisance déterminé indépendamment

Note 1 à l'article: à l'article Le niveau de rigueur dépend de la nature du sujet. Ce terme s'applique uniquement aux actions de l'évaluateur.

3.1.15
connectivité
propriété d'une TOE qui permet des interactions avec des entités TI externes à la TOE

Note 1 à l'article: à l'article Cela comprend les échanges de données par liaison filaire ou non, sur une distance, dans un environnement ou dans une configuration quelconque.

3.1.16
cohérent
relation entre deux entités ou plus qui ne révèle aucune contradiction apparente entre ces entités

3.1.17
contrer
réagir à une attaque de sorte que l'impact d'une menace donnée est atténué mais pas nécessairement éradiqué

3.1.18
conformité démontrable
relation entre une ST et un PP, dans laquelle la ST fournit une solution au problème de sécurité générique dans le PP

Note 1 à l'article: à l'article Le PP et la ST peuvent contenir des instructions totalement différentes qui traitent d'entités différentes, utilisent des entités différentes, etc. Le concept de conformité démontrable convient également pour un type de TOE impliquant l'existence de plusieurs PP similaires, ce qui permet à l'auteur de la ST de revendiquer la conformité à ces PP de façon simultanée, réduisant ainsi la charge de travail.

3.1.19
démontrer
fournir une conclusion tirée d'une analyse moins rigoureuse qu'une «preuve»

3.1.20
dépendance
relation entre des composants, telle que si une exigence basée sur le composant dépendant d'un autre composant est incluse dans un PP, une ST ou un paquet, une exigence basée sur cet autre composant doit normalement être également incluse dans le PP, la ST ou le paquet

3.1.21
décrire
fournir des détails spécifiques d'une entité

3.1.22
déterminer
affirmer une conclusion particulière sur la base d'une analyse indépendante, dans l'objectif de parvenir à une conclusion donnée

Note 1 à l'article: à l'article L'emploi de ce terme implique une analyse véritablement indépendante, en général en l'absence de toute analyse antérieure. À distinguer des termes «confirmer» ou «vérifier», qui impliquent qu'une analyse a déjà été effectuée et qu'elle nécessite une vérification.

3.1.23
environnement de développement
environnement dans lequel la TOE est développée

3.1.24
élément
énoncé indivisible d'un besoin de sécurité

3.1.25
(s')assurer
garantir une solide relation causale entre une action et ses conséquences

Note 1 à l'article: à l'article Lorsque ce terme est précédé du mot «aider», cela indique que la conséquence n'est pas totalement certaine, sur la base de cette seule action.

3.1.26
évaluation
appréciation d'un PP, d'une ST ou d'une TOE par rapport aux critères définis

3.1.27
niveau d'assurance de l'évaluation
ensemble d'exigences d'assurance dérivées de l'ISO/IEC 15408-3, représentant un point sur l'échelle d'assurance prédéfinie par l'ISO/IEC 15408, et qui constituent un paquet d'assurance

3.1.28
autorité d'évaluation
organisation qui définit les normes et surveille la qualité des évaluations menées par des organisations au sein d'une communauté spécifique, et qui met en œuvre l'ISO/IEC 15408 pour les besoins de cette communauté au moyen d'un schéma d'évaluation

3.1.29
schéma d'évaluation
cadre administratif et réglementaire dans lequel est appliquée l'ISO/IEC 15408 par une autorité d'évaluation au sein d'une communauté spécifique

3.1.30
exhaustif
caractéristique d'une approche méthodique adoptée pour effectuer une analyse ou une activité conformément à un plan univoque

Note 1 à l'article: à l'article Ce terme est utilisé dans l'ISO/IEC 15408 en ce qui concerne la conduite d'une analyse ou d'une autre activité. Il est lié au terme «systématique», mais dans un sens considérablement plus fort puisqu'il indique non seulement qu'une approche méthodique a été adoptée pour effectuer l'analyse ou l'activité conformément à un plan univoque, mais également que le plan suivi est suffisant pour s'assurer que toutes les voies possibles ont été exploitées.

3.1.31
expliquer
donner un argument justifiant l'adoption d'un plan d'action

Note 1 à l'article: à l'article Ce terme a un sens différent des termes «décrire» et «démontrer». Il vise à répondre à la question «pourquoi?», sans tenter réellement de défendre l'idée que le plan d'action qui a été entrepris était nécessairement optimal.

3.1.32
extension
ajout à une ST ou à un PP d'exigences fonctionnelles ne figurant pas dans l'ISO/IEC 15408-2 et/ou d'exigences d'assurance ne figurant pas dans l'ISO/IEC 15408-3

3.1.33
entité externe
entité humaine ou TI qui interagit éventuellement avec la TOE en dehors des frontières de la TOE

Note 1 à l'article: à l'article Une entité externe peut également être appelée un utilisateur.

3.1.34
famille
groupement de composants ayant en commun un objectif similaire mais qui diffèrent en termes d'importance ou de rigueur

3.1.35
formel
exprimé dans un langage syntaxique restreint doté d'une sémantique définie basée sur des concepts mathématiques bien établis

3.1.36
guide (d'orientation)
documentation qui décrit la livraison, la préparation, l'exploitation, la gestion et/ou l'utilisation de la TOE

3.1.37
identité
représentation qui identifie de façon unique des entités (par exemple, un utilisateur, un processus ou un disque) dans le contexte de la TOE

Note 1 à l'article: à l'article Une telle représentation peut être une chaîne, par exemple. Dans le cas d'un utilisateur humain, la représentation peut être le nom entier ou abrégé ou un pseudonyme (toujours unique).

3.1.38
informel
exprimé à l'aide d'un langage naturel

3.1.39
transferts inter-TSF
données de communication entre la TOE et les fonctions de sécurité d'autres produits TI de confiance

3.1.40
canal de communication interne
canal de communication qui relie des parties séparées de la TOE

3.1.41
transfert interne à la TOE
données de communication entre parties séparées de la TOE

3.1.42
intrinsèquement cohérent
sans contradictions apparentes entre les différents aspects d'une entité

Note 1 à l'article: à l'article Sur le plan de la documentation, cela signifie que la documentation ne peut pas contenir d'énoncés pouvant être interprétés comme étant mutuellement contradictoires.

3.1.43
itération
utilisation du même composant pour exprimer deux exigences distinctes ou plus

3.1.44
justification
analyse conduisant à une conclusion

Note 1 à l'article: à l'article Une «justification» est plus rigoureuse qu'une démonstration. Ce terme sous-entend une grande rigueur dans l'explication soigneuse et approfondie de chaque étape d'un argument logique.

3.1.45
objet
entité passive dans la TOE, qui contient ou reçoit des informations et sur laquelle les sujets effectuent des opérations

3.1.46
opération
⟨sur un composant de l'ISO/IEC 15408⟩ modification ou répétition d'un composant

Note 1 à l'article: à l'article Les opérations autorisées sur des composants sont l'affectation, l'itération, le raffinement et la sélection.

3.1.47
opération
⟨sur un objet⟩ type spécifique d'action effectuée par un sujet sur un objet

3.1.48
environnement opérationnel
environnement dans lequel la TOE est exploitée

3.1.49
politique de sécurité organisationnelle
ensemble de règles, procédures ou lignes directrices de sécurité pour un organisme

Note 1 à l'article: à l'article Une politique peut être attachée à un environnement opérationnel spécifique.

3.1.50
paquet
ensemble nommé d'exigences fonctionnelles de sécurité ou d'exigences d'assurance de sécurité

Note 1 à l'article: «EAL 3» est un exemple de paquet.

3.1.51
évaluation du profil de protection
appréciation d'un PP par rapport aux critères définis

3.1.52
profil de protection
énoncé des besoins de sécurité indépendant de l'implémentation pour un type de TOE

3.1.53
prouver
montrer une correspondance à l'aide d'une analyse formelle au sens mathématique du terme

Note 1 à l'article: à l'article Cette action est totalement rigoureuse à tous points de vue. En règle générale, le terme «prouver» est utilisé lorsqu'il existe une volonté de montrer une correspondance entre deux représentations de TSF à un niveau de rigueur élevé.

3.1.54
raffinement
ajout de détails à un composant

3.1.55
rôle
ensemble prédéfini de règles établissant les interactions autorisées entre un utilisateur et la TOE

3.1.56
secret
informations qui ne doivent être connues que par des utilisateurs autorisés et/ou par la TSF afin d'appliquer une SFP spécifique

3.1.57
état sécurisé
état dans lequel les données de la TSF sont cohérentes et où la TSF continue d'appliquer correctement les SFR

3.1.58
attribut de sécurité
propriété de sujets, d'utilisateurs (y compris de produits TI externes), d'objets, d'informations, de sessions et/ou de ressources, qui est utilisée pour définir les SFR et dont les valeurs sont utilisées pour appliquer les SFR

3.1.59
politique de sécurité fonctionnelle
ensemble de règles décrivant un comportement de sécurité spécifique appliqué par la TSF et exprimable sous forme d'ensemble de SFR

3.1.60
objectif de sécurité
expression de l'intention de contrer des menaces identifiées et/ou de satisfaire à des politiques de sécurité organisationnelles et/ou à des hypothèses

3.1.61
problème de sécurité
déclaration qui définit de manière formelle la nature et le périmètre de la sécurité que la TOE vise à couvrir

Note 1 à l'article: à l'article Cette déclaration se compose d'une combinaison:

— de menaces devant être contrées par la TOE et son environnement opérationnel;

— des OSP appliquées par la TOE et son environnement opérationnel; et

— des hypothèses retenues pour l'environnement opérationnel de la TOE.

3.1.62
exigence de sécurité
exigence, formulée dans un langage normalisé, qui est supposée contribuer à atteindre les objectifs de sécurité d'une TOE

3.1.63
cible de sécurité
énoncé des besoins de sécurité dépendant de l'implémentation pour une TOE spécifique identifiée

3.1.64
sélection
spécification d'un ou de plusieurs éléments à partir d'une liste au sein d'un composant

3.1.65
semi-formel
exprimé à l'aide d'un langage syntaxique restreint utilisant une sémantique définie

3.1.66
spécifier
fournir des détails spécifiques concernant une entité d'une manière rigoureuse et précise