Norme internationale

ISO/IEC 29146

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'accès

Information technology — Security techniques — A framework for access management

Deuxième édition
2024-01

Numéro de référence
ISO/IEC 29146:2024(fr)

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) 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 organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux.

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. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'ISO et l'IEC attirent 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 et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'ISO et l'IEC n'avaient 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 et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

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/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette deuxième édition annule et remplace la première édition (ISO/IEC 29146:2016), dont elle constitue une révision mineure. Elle incorpore également l'Amendement ISO/IEC 29146:2016/Amd.1:2022. Les modifications sont les suivantes:

— le texte a fait l'objet d'une révision éditoriale et les références normatives ont été mises à jour.

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/members.html et www.iec.ch/national-committees.

Introduction

La gestion de la sécurité de l'information est une tâche complexe qui s'appuie principalement sur une approche de la gestion des risques et qui est soutenue par plusieurs techniques de sécurité. La complexité est traitée par plusieurs systèmes d'appui qui peuvent appliquer automatiquement un ensemble de règles ou de règles de manière régulière.

Dans le cadre de la gestion de la sécurité de l'information, la gestion d'accès joue un rôle clé dans l'administration des relations entre la partie ayant accès (sujets pouvant être des entités humaines ou non) et les ressources des technologies de l'information. Avec le développement de l'Internet, les ressources des technologies de l'information peuvent également être situées sur des réseaux distribués. La gestion d'accès est censée être conforme à une règle et avoir des termes et modèles communs définis dans un cadre.

La gestion de l'identité constitue également une part importante de la gestion d'accès. La gestion d'accès s'effectue par l'identification et l'authentification des parties souhaitant accéder aux ressources des technologies de l'information. La gestion d'accès repose sur l'existence d'un système de gestion de l'identité sous-jacent.

Un cadre pour la gestion de l'accès constitue une partie d'un cadre général de gestion de l'identité et de l'accès. L'autre partie est le cadre pour la gestion de l'identité, défini dans la série ISO/IEC 24760.

Le présent document décrit les concepts, les acteurs, les composants, l'architecture de référence, les exigences fonctionnelles et la pratique d'un cadre de contrôle d'accès.

Le document se concentre principalement sur le contrôle d'accès pour un seul organisme. Il fournit des considérations supplémentaires pour le contrôle d'accès dans les accords de collaboration entre plusieurs organismes. Le document comprend des exemples de modèles de contrôle d'accès.

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'accès

1 Domaine d'application

Le présent document définit et établit un cadre pour la gestion de l'accès (AM, access management) et la gestion sécurisée du processus d'accès à l'information et aux ressources des technologies de l'information et de la communication (TIC), associé à la responsabilité d'un sujet dans certains contextes.

Le présent document fournit des concepts, des termes et des définitions applicables aux techniques de gestion d'accès distribuée dans des environnements en réseau.

Le présent document fournit également des explications concernant l'architecture, les composants et les fonctions de gestion associés.

Les sujets impliqués dans la gestion d'accès peuvent être reconnus de manière unique pour accéder aux systèmes d'information, tel que défini dans la série ISO/IEC 24760.

La nature et les qualités du contrôle d'accès physique intervenant dans les systèmes de gestion d'accès ne relèvent pas du domaine d'application du présent document.

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/IEC 24760-1, *Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre pour la gestion de l'identité — Partie 1: Concepts fondamentaux et terminologie*

ISO/IEC 29115, *Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO/IEC 24760-1 et de l'ISO/IEC 29115 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
contrôle d'accès
autorisation ou refus d'une opération à effectuer sur une *ressource* (3.14)

Note 1 à l'article: Le contrôle d'accès a pour objectif principal d'empêcher l'accès non autorisé aux informations ou l'utilisation non autorisée des ressources des TCI sur la base des exigences métier et de sécurité, c'est-à-dire l'application des règles d'autorisation aux demandes d'accès particulières.

Note 2 à l'article: Lorsqu'un *sujet* (3.15) authentifié effectue une demande, le propriétaire de la ressource autorise (ou non) l'accès conformément à la règle d'accès et aux privilèges du sujet.

3.2
gestion d'accès
ensemble de processus visant à gérer le *contrôle d'accès* (3.1) pour un ensemble de *ressources* (3.14)

3.3
jeton d'accès
objet de confiance qui contient l'autorité permettant à un *sujet* (3.15) d'accéder à une *ressource* (3.14)

Note 1 à l'article: Un jeton d'accès est émis par le point de décision de règle (PDP) et consommé par le point d'application de règle (PEP) pour la ressource.

Note 2 à l'article: Un jeton d'accès peut contenir des informations relatives à l'autorisation d'accès d'un sujet à une ressource et des informations d'identification pour l'autorité de la décision d'autorisation.

Note 3 à l'article: Un jeton d'accès peut contenir des informations permettant la validation de son intégrité.

Note 4 à l'article: Un jeton d'accès peut se présenter sous forme physique ou virtuelle.

3.4
attribut
caractéristique ou propriété utilisée pour décrire et contrôler l'accès à une *ressource* (3.14)

Note 1 à l'article: Les règles d'accès à une ressource sont définies dans une règle de *contrôle d'accès* (3.1) qui spécifie les attributs exigés pour l'autorisation d'accès d'un *sujet* (3.15) à une ressource pour une opération spécifique.

Note 2 à l'article: Les attributs peuvent inclure les attributs du sujet, les attributs de la ressource, les attributs environnementaux et d'autres attributs utilisés pour le contrôle d'accès tel que spécifié dans la règle de contrôle d'accès.

3.5
appareil utilisateur
emplacement dans un système de *gestion d'accès* (3.2) où une fonction de *contrôle d'accès* (3.1) est effectuée

Note 1 à l'article: Les différents types d'appareils utilisateur suivants peuvent exister:

— appareil utilisateur d'authentification, où l'authentification du *sujet* (3.15) est effectuée;

— appareil utilisateur d'autorisation, où l'autorisation du sujet est effectuée;

— service de découverte d'appareil utilisateur, qui recherche et localise les appareils utilisateur;

— service de découverte d'appareil utilisateur initial, utilisé au début des interactions du sujet avec un système de gestion d'accès.

Note 2 à l'article: Les services de découverte d'appareil utilisateur sont généralement utilisés dans les systèmes distribués et en réseau.

3.6
mise en œuvre centrée sur l'entreprise
gestion d'accès (3.2) effectuée sous le contrôle d'un point de décision de règle

3.7
besoin d'en connaître
objectif de sécurité consistant à limiter l'accès du *sujet* (3.15) aux *ressources* (3.14) de données au minimum nécessaire pour permettre à un utilisateur demandeur d'exercer ses fonctions

Note 1 à l'article: Le besoin d'en connaître est autorisé à la discrétion du propriétaire de la ressource.

Note 2 à l'article: Le besoin d'avoir est l'objectif de sécurité du demandeur pour la réalisation de tâches spécifiques susceptibles d'être limitées à la discrétion du propriétaire de la ressource.

3.8
privilège
droit d'accès
autorisation
autorisation octroyée à un *sujet* (3.15) d'accéder à une *ressource* (3.14)

Note 1 à l'article: Le privilège est une condition nécessaire mais non suffisante d'accès. L'accès est permis lorsque la demande d'accès est accordée conformément à sa règle de contrôle d'accès. La règle de contrôle d'accès est fondée sur les privilèges et peut comprendre d'autres facteurs environnementaux (par exemple, heure, localisation, etc.).

Note 2 à l'article: Les privilèges prennent la forme de données présentées par un sujet ou obtenues pour un sujet, qui sont utilisées par un point de décision de règle en vue d'autoriser ou de refuser une opération qu'un sujet souhaite effectuer sur une ressource.

Note 3 à l'article: Une ressource peut être associée à plusieurs privilèges distincts qui correspondent à différents niveaux d'accès définis. Par exemple, une ressource de données peut avoir des privilèges de lecture, d'écriture, d'exécution et de suppression pouvant être attribués aux sujets. Une demande d'accès à la ressource par un sujet peut être autorisée pour certains niveaux de demande d'accès mais refusée pour d'autres niveaux, selon le niveau d'accès demandé et les privilèges de la ressource qui ont été attribués au sujet.

3.9
rôle
nom donné à un ensemble défini de fonctions système pouvant être effectuées par plusieurs entités

Note 1 à l'article: Le nom décrit généralement la fonctionnalité.

Note 2 à l'article: Les entités peuvent être mais ne sont pas nécessairement des sujets humains.

Note 3 à l'article: Les rôles sont mis en œuvre par un ensemble d'attributs de *privilège* (3.8) pour fournir l'accès nécessaire aux ressources de données ou aux objets.

Note 4 à l'article: Les sujets affectés à un rôle héritent des privilèges d'accès associés à ce rôle. Dans le cadre d'une utilisation opérationnelle, les sujets doivent être authentifiés en tant que membres du groupe de rôle avant d'être autorisés à exécuter les fonctions du rôle.

3.10
point de décision de règle
PDP [*policy decision point*]
service qui met en œuvre une règle de contrôle d'accès visant à arbitrer les demandes d'accès à des *ressources* (3.14) provenant d'entités et à fournir des décisions d'autorisation en vue de leur utilisation par un *point d'application de règle* (3.11)

Note 1 à l'article: Les décisions d'autorisation sont utilisées par un point d'application de règle pour contrôler l'accès à une ressource. Une décision d'autorisation peut être communiquée par l'utilisation d'un *jeton d'accès* (3.3).

Note 2 à l'article: Le PDP contrôle également les décisions dans une piste d'audit et est en mesure de déclencher des alarmes.

Note 3 à l'article: Ce terme correspond à «fonction décisionnelle d'accès» (ADF) dans l'ISO/IEC 10181-3. Il est présumé que cette fonction est située sur un réseau à partir du *sujet* (3.15) et qu'elle peut être située sur un réseau à partir du point d'application de règle correspondant.

3.11
point d'application de règle
PEP [*policy enforcement point*]
service qui applique la décision d'accès émise par le *point de décision de règle* (3.10)

Note 1 à l'article: Le PEP reçoit les décisions d'autorisation prises par le PDP et les applique en vue de contrôler l'accès des entités aux *ressources* (3.14). Une décision d'autorisation peut être reçue sous la forme d'un *jeton d'accès* (3.3) présenté par un *sujet* (3.15) lorsqu'une demande d'accès est effectuée.

Note 2 à l'article: Ce terme correspond à «fonction d'application de contrôle d'accès» (AEF) dans l'ISO/IEC 10181-3. Il est présumé que cette fonction est située sur un réseau à partir du sujet et qu'elle peut être située sur un réseau à partir du point de décision de règle correspondant.

3.12
point d'administration de règle
PAP
service qui administre la règle d'autorisation des accès

3.13
point d'information de règle
PIP
service qui agit en tant que source des *attributs* (3.4) utilisés par un *point de décision de règle* (3.10) pour prendre des décisions d'autorisation

Note 1 à l'article: Les attributs peuvent inclure les *privilèges* (3.8)/autorisations des *ressources* (3.14), des *sujets* (3.15) et des environnements.

3.14
ressource
objet
actif physique, réseau ou toute information auxquels un *sujet* (3.15) peut avoir accès pour l'utiliser

3.15
sujet
entité demandant l'accès à une *ressource* (3.14) contrôlée par un système de *contrôle d'accès* (3.1)

3.16
service de jeton de sécurité
STS [*security token service*]
service qui crée, signe, échange et émet des *jetons d'accès* (3.3) sur la base de la décision d'un *point de décision de règle* (3.10)

Note 1 à l'article: Ce service peut être divisé en plusieurs composants.

3.17
mise en œuvre centrée sur le sujet

gestion d'accès (3.2) mise en œuvre sous forme de services de composants appelés par un *sujet* (3.15) pour acquérir les moyens reconnus par le *point d'application de règle* (3.11) afin d'accéder à une *ressource* (3.14)

Note 1 à l'article: Les services de composants peuvent inclure un service de point de décision de règle, un service de point d'application de règle et les services de découverte associés permettant au sujet de localiser et de contacter les services de *contrôle d'accès* (3.1).

4 Abréviations

AA autorité d'attribut

ABAC contrôle d'accès basé sur les attributs [*attribute-based access control*]

AM gestion d'accès [*access management*]

AMS système de gestion d'accès [*access management system*]

CBAC contrôle d'accès basé sur les capacités [*capabilities-based access control*]

DAC contrôle d'accès discrétionnaire [*discretionary access control*]

DCP données à caractère personnel

IBAC contrôle d'accès basé sur l'identité [*identity-based access control*]

IMS système de gestion de l'identité [*identity management system*]

LCA liste de contrôle d'accès

MAC contrôle d'accès obligatoire [*mandatory access control*]

PAP point d'administration de règle

PBAC contrôle d'accès basé sur le pseudonyme [*pseudonym-based access control*]

PDP point de décision de règle

PEP point d'application de règle [*policy enforcement point*]

PIP point d'information de règle

RBAC contrôle d'accès basé sur le rôle [*role-based access control*]

REDS service de découverte d'appareil utilisateur de ressource [*resource endpoint discovery service*]

STS service de jeton de sécurité [*security token service*]

TI technologie de l'information

TIC technologie de l'information et de la communication

TLS sécurité de la couche de transport [*transport layer security*]

XACML langage XML de contrôle d'accès [*extensible access control markup language*]

5 Concepts

5.1 Modèle de contrôle d'accès aux ressources

5.1.1 Vue d'ensemble

La séquence conceptuelle de l'octroi de l'accès à une ressource est comme suit.

a) L'authentification du sujet est nécessaire avant l'octroi de l'accès à une ressource. Toutefois, l'authentification est une fonction distincte qui est généralement mise en œuvre sur la base d'une session plutôt que pour chaque demande d'accès.

b) La décision d'autorisation ou de refus de l'accès à la ressource est prise sur la base d'une règle, et un jeton d'accès est émis pour transmettre le résultat de la décision.

c) L'autorisation est appliquée sur la ressource sur la base du résultat de la décision et l'accès à la ressource est octroyé.

La Figure 1 présente cette séquence de décision.

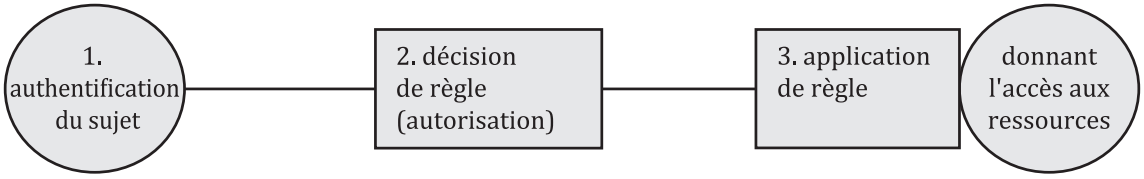

Figure 1 — Séquence du modèle de contrôle d'accès

Le sujet et la ressource sont représentés par des bulles et les fonctions conceptuelles par des rectangles.

Afin de pouvoir être accessible, une ressource est caractérisée par les éléments suivants:

— un identifiant, pour une classe spécifique ou pour une classe de ressource;

— un ou plusieurs modes d'accès;

— un ensemble d'attributs associés aux modes d'accès et à d'autres critères d'accès tels que spécifiés dans la règle de contrôle d'accès.

Un système de gestion d'accès est responsable de l'administration et du fonctionnement des autorisations d'accès. Les autorisations sont soutenues par l'activité d'administration qui affecte et gère les attributs des ressources et les privilèges des sujets conformément à la règle de gestion d'accès.

Les ressources dans les systèmes informatiques sont généralement dynamiques. Elles ont un cycle de vie allant de leur création à leur destruction dans un processus continu.

a) Les ressources ont un cycle de vie allant de leur création à leur destruction.

b) Les ressources sont créées, mises à jour et détruites de façon continue.

c) Il est nécessaire d'affecter aux ressources des attributs d'accès (généralement lors de leur création) qui sont utilisés par le système de gestion d'accès pour contrôler l'accès des sujets aux ressources. [Pour ce faire, des types de ressources sont généralement prédéfinis avec des modèles d'attributs d'accès associés. À la création d'une ressource de type connu, celle-ci hérite des attributs d'accès du modèle correspondant.]

d) Les ressources sont détenues par une partie qui peut être une personne ou un organisme. Le propriétaire est souvent, mais pas toujours, le créateur de la ressource et la propriété est susceptible d'évoluer au cours de la vie de la ressource.

5.1.2 Relation entre le système de gestion de l'identité et le système de gestion d'accès

Dans le modèle décrit ici, le sujet est authentifié à l'aide d'un système de gestion de l'identité (IMS), tel que décrit dans l'ISO/IEC 24760-2. Le sujet authentifié demande ensuite l'accès à l'aide du système de gestion d'accès (AMS). Le système de gestion d'accès détermine s'il autorise ou non la demande d'accès à la ressource par le sujet. L'autorisation du sujet comprend deux activités distinctes:

— la pré-attribution aux sujets des privilèges d'accès aux ressources; et

— l'autorisation de l'accès aux ressources par les sujets en utilisation opérationnelle.

La Figure 2 présente la relation entre un système de gestion de l'identité et un système de gestion d'accès.

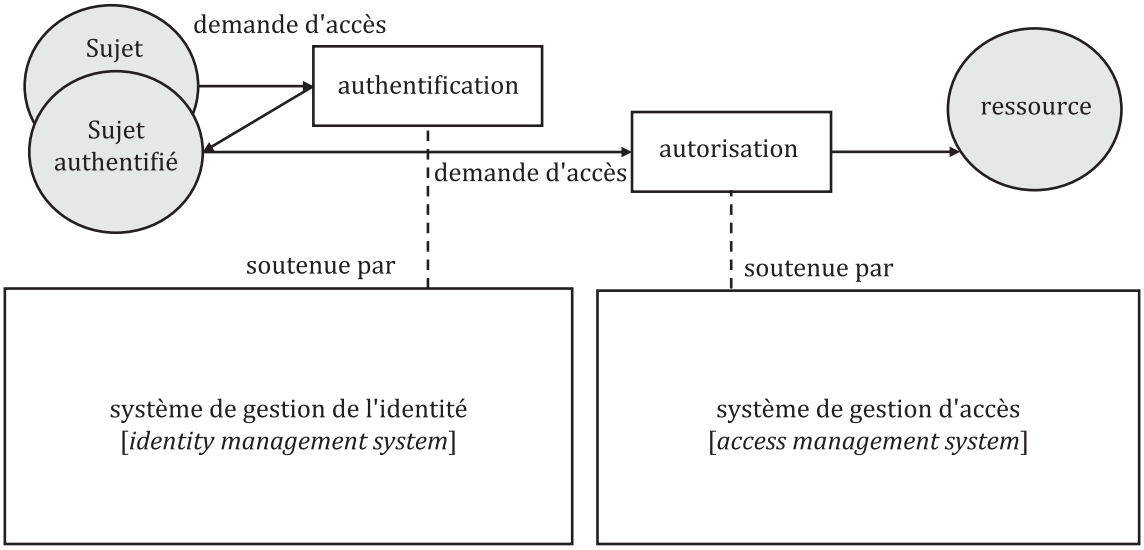

Figure 2 — Relation entre le système de gestion de l'identité et le système de gestion d'accès