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

*Information technology — Security techniques — A framework for
access management*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 29146:2016](https://standards.iteh.ai/catalog/standards/sist/b10cdb1e-0188-4b8e-bc7d-ae76628649ab/iso-iec-29146-2016)

[https://standards.iteh.ai/catalog/standards/sist/b10cdb1e-0188-4b8e-bc7d-
ae76628649ab/iso-iec-29146-2016](https://standards.iteh.ai/catalog/standards/sist/b10cdb1e-0188-4b8e-bc7d-ae76628649ab/iso-iec-29146-2016)



iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 29146:2016

<https://standards.iteh.ai/catalog/standards/sist/b10cdb1e-0188-4b8e-bc7d-ae76628649ab/iso-iec-29146-2016>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2016

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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	v
Introduction	vi
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Abréviations	4
5 Concepts	5
5.1 Modèle de contrôle d'accès aux ressources	5
5.1.1 Vue d'ensemble	5
5.1.2 Relation entre le système de gestion de l'identité et le système de gestion d'accès	6
5.1.3 Caractéristiques de sécurité de la méthode d'accès	7
5.2 Relations entre le contrôle d'accès logique et physique	8
5.3 Fonctions et processus du système de gestion d'accès	8
5.3.1 Vue d'ensemble	8
5.3.2 Règle de contrôle d'accès	9
5.3.3 Gestion des privilèges	10
5.3.4 Gestion des informations sur les attributs liés aux règles	11
5.3.5 Autorisation	12
5.3.6 Gestion de la surveillance	13
5.3.7 Gestion des alarmes	14
5.3.8 Contrôle d'accès fédéré	14
6 Architecture de référence	15
6.1 Vue d'ensemble	15
6.2 Composants de base d'un système de gestion d'accès	16
6.2.1 Appareil utilisateur d'authentification	16
6.2.2 point de décision de règle (PDP)	16
6.2.3 Point d'information de règle (PIP)	16
6.2.4 Point d'administration de règle (PAP)	16
6.2.5 Point d'application de règle (PEP)	17
6.3 Composants de services supplémentaires	17
6.3.1 Généralités	17
6.3.2 Mise en œuvre centrée sur le sujet	17
6.3.3 Mise en œuvre centrée sur l'entreprise	19
7 Exigences et enjeux supplémentaires	20
7.1 Accès aux informations administratives	20
7.2 Modèles d'AMS et enjeux de règle	20
7.2.1 Modèles de contrôle d'accès	20
7.2.2 Règles dans la gestion d'accès	21
7.3 Exigences légales et réglementaires	21
8 Mise en œuvre	22
8.1 Processus	22
8.1.1 Processus d'autorisation	22
8.1.2 Processus de gestion des privilèges	22
8.2 Menaces	23
8.3 Objectifs des mesures	24
8.3.1 Généralités	24
8.3.2 Validation du cadre de gestion d'accès	24
8.3.3 Validation du système de gestion d'accès	26
8.3.4 Validation de la maintenance d'un AMS mis en œuvre	30
Annexe A (informative) Modèles d'accès actuels	33

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 29146:2016

<https://standards.iteh.ai/catalog/standards/sist/b10cdb1e-0188-4b8e-bc7d-ae76628649ab/iso-iec-29146-2016>

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. 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 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'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. 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'Organisation mondiale du commerce (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/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité de l'information*.

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 être situées sur des réseaux distribués et l'accès à ces ressources doit être géré conformément à une règle, et il est attendu que des termes et des modèles communs servent de cadre pour la gestion de l'accès.

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 sujets souhaitant accéder aux ressources des technologies de l'information. La présente Norme internationale dépend de l'existence d'un système de gestion de l'identité sous-jacent ou d'une infrastructure de gestion de l'identité (voir les références à l'[Article 2](#)).

Le 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 l'ISO/IEC 24760.

La présente Norme internationale décrit les concepts, les acteurs, les composants, l'architecture de référence, les exigences fonctionnelles et les pratiques pour le contrôle d'accès. Des exemples de modèles de contrôle d'accès sont inclus.

Elle se concentre principalement sur le contrôle d'accès pour un seul organisme, mais elle ajoute d'autres considérations pour le contrôle d'accès dans les accords de collaboration entre plusieurs organismes.

[ISO/IEC 29146:2016](https://standards.iteh.ai/catalog/standards/sist/b10cdb1e-0188-4b8e-bc7d-ae76628649ab/iso-iec-29146-2016)

<https://standards.iteh.ai/catalog/standards/sist/b10cdb1e-0188-4b8e-bc7d-ae76628649ab/iso-iec-29146-2016>

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

1 Domaine d'application

La présente Norme internationale 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 un certain contexte.

La présente Norme internationale fournit des concepts, des termes et des définitions applicables aux techniques de gestion d'accès distribuée dans des environnements en réseau.

La présente Norme internationale 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 l'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 de la présente Norme internationale.

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application 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 24760-1:2011, *Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité — Partie 1: Terminologie et concepts*

ISO/IEC 24760-2:2015, *Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité — Partie 2: Architecture de référence et exigences*

ISO/IEC 29115:2013, *Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité*

ISO/IEC 27002:2013, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO/IEC 24760-1 et de l'ISO/IEC 29115 ainsi que les suivants, s'appliquent.

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 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 *PEP* (3.11) 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 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 *PDP* (3.10) 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/autorisations* (3.8) 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 [<i>access management</i>]
AMS	système de gestion d'accès [<i>access management system</i>]
CBAC	contrôle d'accès basé sur les capacités [<i>capabilities-based access control</i>]
DAC	contrôle d'accès discrétionnaire [<i>discretionary access control</i>]
DCP	données à caractère personnel
IBAC	contrôle d'accès basé sur l'identité [<i>identity-based access control</i>]
IMS	système de gestion de l'identité [<i>identity management system</i>]
LCA	liste de contrôle d'accès
MAC	contrôle d'accès obligatoire [<i>mandatory access control</i>]
PAP	point d'administration de règle
PBAC	contrôle d'accès basé sur le pseudonyme [<i>pseudonym-based access control</i>]
PDP	point de décision de règle
PEP	point d'application de règle [<i>policy enforcement point</i>]
PIP	point d'information de règle
RBAC	contrôle d'accès basé sur le rôle [<i>role-based access control</i>]
REDS	service de découverte d'appareil utilisateur de ressource [<i>resource endpoint discovery service</i>]
STS	service de jeton de sécurité [<i>security token service</i>]
TI	technologie de l'information
TIC	technologie de l'information et de la communication
TLS	sécurité de la couche de transport [<i>transport layer security</i>]
XACML	langage XML de contrôle d'accès [<i>extensible access control markup language</i>]

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.

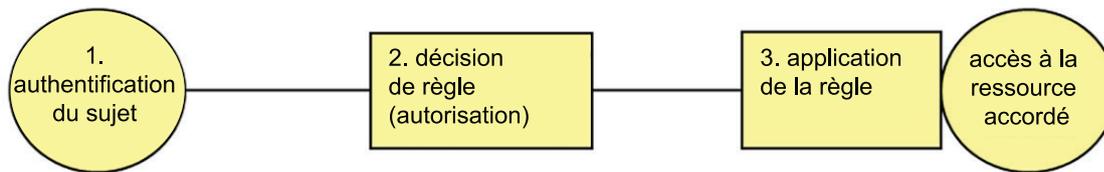


Figure 1 — Séquence du modèle de contrôle d'accès

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 (IMS) et un système de gestion d'accès (AMS).

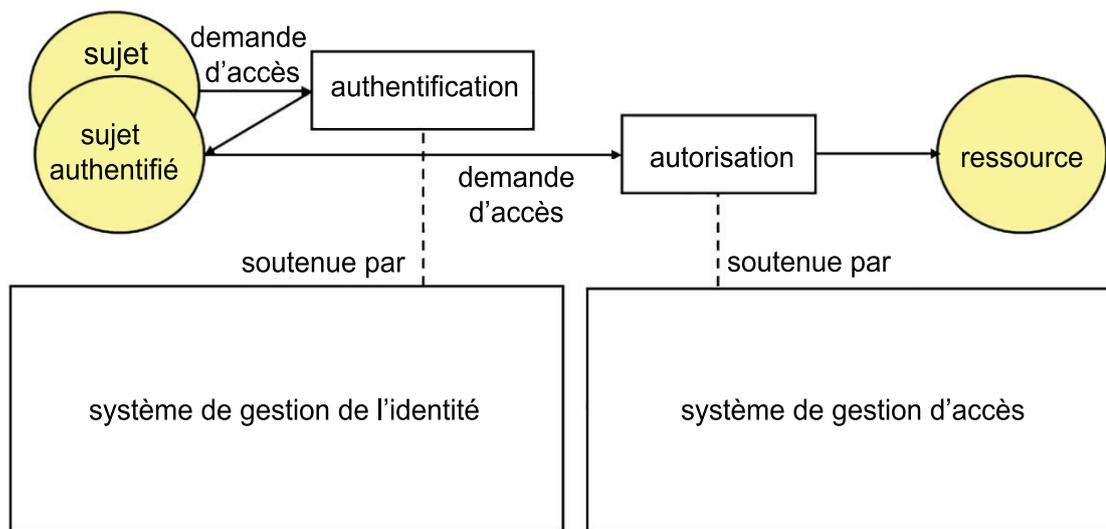


Figure 2 — Relation entre le système de gestion de l'identité et le système de gestion d'accès

L'authentification est soutenue par un système de gestion de l'identité (IMS). Dans un système de gestion d'accès utilisant le modèle IBAC, l'identité est la base de l'attribution aux sujets des privilèges d'accès aux ressources et de l'autorisation des demandes d'accès aux ressources par les sujets en utilisation opérationnelle.

NOTE L'autorisation de l'accès à une ressource peut exiger un niveau défini minimal d'assurance de l'authentification du sujet en fonction du profil de risque de la ressource. Le niveau exigé dépend du risque lié à l'identité relatif à la ressource faisant l'objet d'une demande d'accès. Pour de plus amples informations sur le niveau d'assurance de l'authentification, voir l'ISO/IEC 29115.

L'autorisation est fournie par le système de gestion d'accès (AMS) qui assure la gestion des informations d'accès.

La pratique de mise en œuvre pour les systèmes de gestion d'accès peut varier selon l'architecture et le modèle de contrôle d'accès utilisés, par exemple:

- lorsqu'un AMS est mis en œuvre en tant que système de services Web, un sujet peut demander l'accès à une ressource sans authentification préalable. Dans ce cas, l'AMS invite le sujet à demander à l'IMS de fournir une authentification; et
- lorsqu'un modèle ABAC est adopté, il est possible qu'aucune authentification ne soit exigée de la part d'un sujet. Dans ce cas, une entité anonyme peut être autorisée à s'adresser directement à l'AMS et la décision d'autorisation est prise sur la base d'un justificatif d'identité qui peut être validé afin de prouver que le sujet possède les attributs déclarés.

5.1.3 Caractéristiques de sécurité de la méthode d'accès

Il convient de prendre en compte les aspects liés à la sécurité de la mise en œuvre et des processus des systèmes de contrôle d'accès, en particulier lorsque des architectures fédérées sont utilisées.

Pour des raisons de sécurité, il peut être nécessaire de d'abord valider l'intégrité de la demande d'accès avant que celle-ci ne soit traitée par le système de gestion d'accès.

Lorsque les canaux de communication sont fiables, comme dans le cas des connexions privées au sein d'un organisme, une protection supplémentaire peut ne pas être nécessaire. Toutefois, lorsque les canaux de communication empruntent des réseaux publics ou d'autres canaux non protégés, il convient de prévoir des mesures visant à protéger l'intégrité et la confidentialité des demandes d'accès et des données associées pour la demande d'accès elle-même (privilèges, données d'authentification du sujet,