IEC 62351-8

Edition 2.0 2026-07

NORME INTERNATIONALE

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 8: Contrôle d'accès basé sur les rôles pour la gestion de systèmes de puissance

ICS 33.200

ISBN 978-2-8327-1354-9

IEC 62351-8:2026-07(fr)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 8: Contrôle d'accès basé sur les rôles pour la gestion de systèmes de puissance

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend 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'IEC avait 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 https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62351-8 a été établie par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés. Il s'agit d'une Norme internationale.

Cette deuxième édition annule et remplace la première édition parue en 2020. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) Suppression de la mise en correspondance des rôles avec les permissions pour les objets selon le modèle de données et/ou le protocole cible pour permettre d'autres mises en correspondance que celles de l'IEC 61850. La mise en correspondance est déléguée à des documents distincts;
b) Spécification du traitement d'une combinaison de rôles et de permissions en tant qu'operationSet pour permettre des affectations plus fines aux objets;
c) Spécification d'une affectation simplifiée des rôles pour traiter plus efficacement les situations dans lesquelles les rôles sont utilisés en relation avec différents modèles de données, y compris des exemples;
d) Inclusion d'un nouveau profil pour permettre de récupérer des informations RBAC à partir de référentiels LDAP;
e) Définition d'événements de sécurité spécifiques dans l'ensemble du document;
f) Alignement de la terminologie et renforcement avec des exemples.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
57/2882/FDIS	57/2921/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

Les destinataires du présent document sont invités à présenter, avec leurs observations, la notification des droits de propriété dont ils auraient éventuellement connaissance et à fournir une documentation explicative.

Le présent document comprend des composants de code, c'est-à-dire des composants destinés à être directement traités par un ordinateur. Les éléments de code sont représentés par du texte placé entre les marqueurs <CODE BEGINS> et <CODE ENDS>, ou sont clairement identifiés en tant qu'éléments de code dans le présent document.

Sinon, ils sont clairement indiqués dans le présent document comme composants de code. L'achat du présent document IEC est accompagné d'une licence de copyright permettant à l'acheteur de vendre des logiciels contenant les composants de code du présent document aux utilisateurs finaux, directement ou par l'intermédiaire de distributeurs soumis aux conditions de licence des logiciels IEC, qui peuvent être consultées à l'adresse: http://www.iec.ch/CCv1.

Dans le cas d'une divergence entre le document les composants de code, les composants de code prévalent.

Dans le présent document, les caractères d'imprimerie suivants sont utilisés:

Codage en ASN.1 ou XACML: `couriernew`

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

– reconduit,
– supprimé, ou
– révisé.

INTRODUCTION

Le présent document est une norme qui fournit les exigences relatives au contrôle d'accès dans les systèmes de puissance. L'environnement de systèmes de puissance pris en charge par le présent document est à l'échelle de l'entreprise et s'étend au-delà des limites traditionnelles pour comprendre les fournisseurs externes, les prestataires et les autres partenaires énergétiques. Les éléments moteurs sont la libéralisation du secteur énergétique pour comprendre davantage de parties prenantes, la décentralisation progressive de la production d'énergie et le besoin de contrôle d'accès aux données sensibles relatives aux ressources et aux parties prenantes.

Le secteur des systèmes de puissance améliore de manière continue la fourniture d'énergie en tirant profit des avancées technologiques des applications informatiques. Les opérateurs d'entreprises d'électricité, les acheteurs d'énergie et les utilisateurs finaux accèdent de plus en plus à de multiples applications lorsqu'il s'agit de fournir, transmettre et consommer de l'énergie de manière personnalisée. Ces applications disparates sont naturellement raccordées à une infrastructure commune de réseaux qui prend généralement en charge les dispositifs de protection, les protocoles d'automatisation de poste, les protocoles entre postes, les accès à distance et les services interentreprises. Par conséquent, les accès sécurisés à ces applications distribuées et souvent couplées de manière souple sont encore plus importants que les accès à une application en cours d'exécution sur un dispositif autonome.

L'accès sécurisé aux applications informatiques implique l'authentification de l'utilisateur pour l'application. Après l'authentification, les types d'interactions que cet utilisateur peut avoir avec l'application sont déterminés. L'utilisation de mécanismes locaux d'autorisation engendre une multitude d'approches disparates difficiles à gérer de manière uniforme à tous les niveaux d'une entreprise de systèmes de puissance. Chaque application décide, avec sa propre logique, du processus d'autorisation. Cependant, si les applications peuvent utiliser un réseau en vue de faciliter la gestion de l'accès, une base de données peut être utilisée comme une source de confiance de groupe d'utilisateurs ou d'affiliation de rôle. Par conséquent, l'accès à une base partagée d'utilisateurs peut être commandé de manière centrale. Chaque application peut ensuite examiner les permissions énumérées pour un sujet et le rôle correspondant et déterminer leur niveau d'autorisation.

Le présent document définit les contrôles d'accès basés sur les rôles (RBAC – role-based access control) pour les usages à tous les niveaux d'une entreprise dans les systèmes de puissance. Il prend en charge une architecture distribuée ou orientée service dans laquelle la sécurité est un service distribué et les applications sont les consommatrices des services distribués.

Dans le présent document, le rôle d'un utilisateur est contenu dans une structure de données, appelée "jeton d'accès" pour cet utilisateur et est fourni à la ressource à laquelle il accède. Les jetons d'accès sont créés et gérés par un outil de gestion d'identités (éventuellement fédéré). Tous les jetons d'accès ont une durée de vie et sont soumis à expiration. Avant la vérification du jeton d'accès proprement dit, l'utilisateur qui tente d'obtenir l'accès est authentifié par la ressource. La ressource a une relation de confiance avec la gestion du jeton d'accès. Le jeton d'accès peut être fourni en tant qu'objet autonome par l'utilisateur ou un référentiel central, ou en tant que structure de données par un référentiel central. Plus précisément, le jeton d'accès autonome permet de vérifier localement la validité du jeton d'accès sur des sites distants sans qu'il soit nécessaire d'accéder à un référentiel centralisé. Pour assurer la disponibilité des informations dans le référentiel, la redondance peut être envisagée. À noter que les concepts de redondance n'entrent pas dans le champ d'application du présent document.

Différents formats de jetons d'accès sont pris en charge comme cinq profils définis. Ces jetons d'accès peuvent être liés à un transport spécifique ou à une application spécifique conjointement avec différents types de référentiels, contenant les jetons d'accès. Les informations contenues permettant la migration d'un profil à un autre sont communes à tous les profils.

Étant donné que le système RBAC est en cours d'adoption pour plusieurs protocoles et modèles de données, le présent document a été modifié en conséquence. Dans sa version actuelle, il se concentre sur la définition générale de RBAC, sur les rôles obligatoires à prendre en charge et sur les options d'affectation des rôles aux permissions. L'affectation réelle des rôles aux permissions et, par conséquent, la liaison des informations relatives au RBAC avec les objets sont traitées dans les documents de référence, qui se rapportent directement au modèle de données cible. La définition existante des rôles et permissions spécifiques à l'IEC 61850 a été déplacée vers l'IEC 61850-90-19. De même pour l'IEC 60807-5-101/-104, les spécificités sont traitées dans l'IEC 60870-5-7:2025. De plus, les spécificités de l'IEEE 1815 sont traitées dans le contexte de DNP3SAv6. Le présent document fournit des informations sur l'affectation des rôles et des permissions des versions précédentes du document dans l'Annexe B.

La présente norme est maintenue. Les questions techniques identifiées après publication sont traitées par le biais de la base de données TISSUE afin de conserver l'exactitude et l'interopérabilité. Les questions techniques approuvées sont publiées en tant que document INF et peuvent être traitées ultérieurement conformément aux directives de l'IEC.

1 Domaine d'application

1.1 Généralités

La présente partie de l'IEC 62351 a pour objet de faciliter le contrôle d'accès basé sur les rôles (RBAC) pour la gestion de systèmes de puissance. Le RBAC attribue des utilisateurs humains, des systèmes automatisés et des applications logicielles (appelés "sujets" dans le présent document) aux "rôles" spécifiés et limite leur accès à ces ressources uniquement, que les politiques de sécurité identifient comme nécessaires à leurs rôles.

Les systèmes électriques de puissance étant de plus en plus automatisés et les préoccupations relatives à la cybersécurité étant de plus en plus importantes, il est de plus en plus critique d'assurer la restriction de l'accès aux données (lecture, écriture, contrôle, etc.). Comme pour beaucoup d'aspects liés à la sécurité, le RBAC n'est pas uniquement une technologie; il s'agit d'une manière de diriger une entreprise. Le RBAC n'est pas un concept nouveau; en réalité, il est utilisé par de nombreux systèmes d'exploitation pour contrôler l'accès aux ressources de systèmes. Le RBAC fournit notamment une alternative au modèle tout ou rien de super utilisateur dans lequel tous les sujets ont accès à toutes les données, y compris aux commandes de contrôle.

Le RBAC est une méthode primaire pour satisfaire au principe de sécurité de moindre privilège, qui indique qu'il convient qu'aucun sujet ne se voit attribué plus de permissions que nécessaire pour effectuer la tâche affectée audit sujet. Avec le RBAC, l'autorisation est distincte de l'authentification. Le RBAC permet à une organisation de subdiviser les capacités des super-utilisateurs et de les regrouper dans des comptes d'utilisateurs spéciaux, appelés rôles, pour les attribuer à des personnes spécifiques en fonction des responsabilités qui leur sont associées. Cette sous-division permet aux politiques de sécurité de déterminer les personnes ou les systèmes qui ont accès aux données dans d'autres systèmes. Le RBAC fournit ainsi un moyen de réattribuer des contrôles de systèmes comme cela est défini par la politique organisationnelle. Le RBAC peut notamment protéger des opérations sensibles de systèmes contre des actions commises par inadvertance (ou délibérées) par des utilisateurs non autorisés. Cependant, le RBAC ne se limite clairement pas aux utilisateurs humains; il s'applique tout aussi bien aux systèmes automatisés qu'aux applications logicielles, c'est-à-dire, aux parties logicielles qui fonctionnent indépendamment des interactions avec l'utilisateur.

Les interactions suivantes relèvent du domaine d'application:

– accès local (raccordé directement) à l'objet par un utilisateur humain, un agent ordinateur automatisé local, ou à l'aide de l'IHM ou du panneau intégré(e) aux objets;

– accès à distance (par ligne commutée ou support sans fil) à l'objet par un utilisateur humain;

– accès à distance (par ligne commutée ou support sans fil) à l'objet par un agent ordinateur automatisé distant, par exemple, un autre objet dans un autre poste, une ressource d'énergie distribuée dans l'installation d'un utilisateur final, ou une application centrale de contrôle.

Tandis que le présent document définit un ensemble de rôles obligatoires à prendre en charge, le format d'échange de rôles définis spécifiques ou personnalisés relève également du domaine d'application du présent document. Pour ce faire, deux approches de codage différentes sont définies pour traiter la définition des rôles personnalisés, soit selon des permissions spécifiques, soit selon des contraintes imposées aux permissions existantes. La définition du traitement des rôles personnalisés a été lancée dans l'IEC 62351-90-1 et reprise dans l'IEC 62351-8:2020. En outre, en plus de la définition de rôles personnalisés fondée sur les permissions associées, le présent document inclut également des options sur la manière d'attribuer les permissions aux objets de manière générale. Les documents de référence fournissent une correspondance avec un modèle de données concret pour assurer l'interopérabilité des rôles normalisés utilisés dans différents modèles de données, ainsi que des rôles personnalisés. Les documents de référence peuvent être des normes telles que l'IEC PAS 61850-90-19 ou l'IEC 60870-5-7:2025, ou encore des définitions établies par un opérateur.

Tous les thèmes non directement liés à la définition des rôles et des jetons d'accès concernant les accès locaux et distants, en particulier les tâches administratives ou organisationnelles, ne relèvent pas du domaine d'application du présent document. Ils incluent, entre autres:

– définition des noms d'utilisateurs et définitions/stratégies de mots de passe;
– gestion de clés et/ou échange de clés;
– processus d'ingénierie des rôles;
– attribution des rôles;
– choix des autorités de certification de confiance émettant des justificatifs d'identité (jetons d'accès);
– définition des tâches d'un responsable de la sécurité;
– intégration de politiques locales dans le RBAC.

NOTE La gestion de certificats est spécifiquement traitée dans l'IEC 62351-9.

Les normes existantes (voir ANSI INCITS 359-2004, IEC 62443 (toutes les parties), et IEEE 802.1X-2020) relatives à l'industrie du contrôle de processus et au contrôle d'accès (RFC 2904 et RFC 2905) ne suffisent pas pour traiter les spécificités de l'automatisation des systèmes de puissance, car aucune d'entre elles ne spécifie le nom de rôle exact et les permissions associées ou le format des jetons d'accès ou encore le mécanisme détaillé par lequel les jetons d'accès sont transférés au système cible et authentifiés par celui-ci. Le présent document aborde cette question en définissant le format des jetons d'accès, leur distribution et leur vérification à partir de la technologie existante.

Dans l'ensemble du document, des événements de sécurité sont définis. Ces événements de sécurité sont destinés à prendre en charge la gestion des erreurs et à augmenter ainsi la résilience d'un système. Il est nécessaire que les mises en œuvre fournissent un mécanisme pour annoncer les événements de sécurité.

Les informations relatives aux événements de sécurité et les informations détaillées potentielles peuvent uniquement être fournies par l'entité en fonction de la disponibilité de ces informations par l'intermédiaire de la plateforme sous-jacente ou des composants utilisés.

Il est fortement recommandé que les événements de sécurité définis dans le document soient rendus accessibles à l'infrastructure opérationnelle par les événements de cybersécurité spécifiés dans l'IEC 62351-14 et/ou par la surveillance des objets comme cela est spécifié dans l'IEC 62351-7. Annexe A présente une correspondance entre les événements définis dans le présent document et la notion de l'IEC 62351-14.

Les avis, les avertissements, les erreurs et les alarmes sont utilisés pour indiquer la sévérité d'un événement du point de vue de la sécurité. La notion suivante de l'IEC 62351-14 est utilisée:

– Un *avis* fait référence à une activité liée à la cybersécurité pendant l'utilisation ou la maintenance courante d'une entité. Il ne concerne pas une atteinte à la sécurité informatique, une attaque ou une déviation par rapport aux conditions de fonctionnement normal d'une entité.
– Un *avertissement* est une déviation par rapport aux conditions de fonctionnement normal d'une entité, mais il ne s'agit pas nécessairement d'une cyberattaque.
– Une *erreur* décrit une condition imprévue, qui peut indiquer une activité non autorisée. Elle peut ne pas exiger une action immédiate.
– Une *alarme* est l'indication d'un problème grave, qui peut indiquer une activité non autorisée. Il est prévu que des mesures soient prises immédiatement.

Il est, en toute circonstance, prévu qu'une politique de sécurité de l'organisation détermine le traitement final des événements selon l'environnement opérationnel. Par exemple, l'évaluation d'une ou de plusieurs alarmes peut atteindre le niveau d'un incident.

1.2 Versions publiées de la norme et nom d'espace de nom associé

Le Tableau 1 fournit une référence entre toutes les éditions publiées, tous les amendements ou corrigenda de ce document et le nom complet de l'espace de nom.

Tableau 1 – Versions publiées et nom d'espace de nom associé

Édition	Date de publication	Webstore	Espace de nom
Édition TS 1.0	2011-09	IEC 62351-8:2011	
Édition IS 1.0	2020-04	IEC 62351-8:2020	
Édition IS 2.0	2026-07	IEC 62351-8:2026	

1.3 Identification de l'élément de code

Les éléments de code associés au présent document sont des exemples XACML dans des fichiers XML pour la définition des rôles personnalisés, des exemples de schémas LDAP dans des fichiers LDIF, ainsi que les définitions des jetons d'accès RBAC pour les profils A et B dans un fichier ASN et pour le profil C dans un fichier JSON.

Les paramètres qui identifient les éléments de code sont fournis dans le Tableau 2:

Tableau 2 – Attributs de l'élément de code de l'IEC 62351-8

Attribut	Contenu
Version	2026
Révision	A
Édition	1
Nom de l'élément de code	IEC_62351-8.ASN1-JSON-XACML-LDIF-Examples.2026A.full.IS

À noter que les éléments de code ne fournissent pas d'espace de nom propre et s'appuient plutôt sur les espaces de noms XACML définis dans la spécification W3C associée.

1.4 Distribution des éléments de code

Chaque élément de code est un paquetage ZIP, qui contient une représentation électronique de l'élément de code lui-même, avec un fichier descriptif du contenu du paquetage (IECManifest.xml).

Le cycle de vie d'un élément de code n'est pas limité au cycle de vie de la publication associée. Le cycle de vie de la publication passe par deux étapes, la Version (qui correspond à une édition) et la Révision (qui correspond à un amendement). Une troisième étape de publication (Édition) permet de publier un élément de code pour apporter des corrections urgentes aux InterOp Tissues, sans nécessiter la publication d'un amendement.

Par conséquent, plusieurs nouvelles éditions de l'élément de code peuvent être éditées, lesquelles annulent et remplacent l'édition précédente et sont distribuées sur le site web du CE 57 de l'IEC à l'adresse:

https://www.iec.ch/tc57/supportdocuments

La dernière version/édition de l'élément de code se trouve en choisissant le fichier de l'élément de code avec la valeur la plus élevée de VersionStateInfo, par exemple IEC_62351-8.ASN1-JSON-XACML-LDIF-Examples.{VersionStateInfo}.full.zip.