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



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2026 IEC, Geneva, Switzerland

Droits de reproduction réservés. Sauf indication contraire, 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 et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

AVANT-PROPOS 6
INTRODUCTION 9
1 Domaine d'application 11
1.1 Généralités 11
1.2 Versions publiées de la norme et nom d'espace de nom associé 13
1.3 Identification de l'élément de code 13
1.4 Distribution des éléments de code 13
2 Références normatives 14
3 Termes et définitions 15
4 Abréviations 18
5 RBAC – Modèle de processus et concepts 19
5.1 Généralités 19
5.2 Vue d'ensemble du modèle de processus RBAC 20
5.3 Concepts génériques de RBAC 20
5.4 Séparation des sujets, rôles et permissions 22
5.4.1 Modèle de RBAC 22
5.4.2 Affectation de sujet (mise en correspondance sujet-rôle) 25
5.4.3 Mise en correspondance rôle-permission 26
5.4.4 Définition des permissions 26
5.4.5 Affectation `operationSet` (mise en correspondance de combinaisons rôles-permissions avec des objets) 26
5.5 Critères de définition des rôles 27
5.5.1 Politiques 27
5.5.2 Sujets, rôles et permissions 27
5.5.3 Réduction de la complexité par l'introduction de rôles 27
6 Définition des rôles et affectation des permissions 28
6.1 Généralités 28
6.2 Rôles prédéfinis 28
6.3 Affectation rôle-permission 29
6.3.1 Généralités 29
6.3.2 Nombre de permissions prises en charge par un rôle 30
6.3.3 Nombre de rôles pris en charge 30
6.3.4 Affectation des permissions aux rôles 30
6.4 Définition des rôles prédéfinis et personnalisés 33
6.4.1 Généralités 33
6.4.2 Codage des rôles en fonction des permissions spécifiques 34
6.4.3 Codage des rôles à l'aide de contraintes sur les permissions existantes 40
6.5 Prise en compte des états opérationnels 43
6.6 Prise en compte des événements de sécurité pour l'ingénierie des rôles et des permissions 44
7 Affectation simplifiée des rôles 46
7.1 Généralités 46
7.2 Application de rôles associés à des définitions de rôles multiples (rôles génériques) 46
7.3 Exemples illustratifs 48
7.3.1 Généralités 48

7.3.2 Application du rôle prédéfini "VIEWER" sur le Device-X pour toutes les définitions de rôles 48
7.3.3 Application du rôle personnalisé "OPERATOR-DFR" sur le Device-Y pour toutes les définitions de rôles prises en charge 49
7.3.4 Application du rôle prédéfini "SECADM" aux définitions de rôles sélectionnées 50
8 Définition des jetons d'accès 52
8.1 Généralités 52
8.2 Profils pris en charge 52
8.3 Identificateurs d'objets liés au contrôle d'accès basé sur les rôles 52
8.4 Structure générale des jetons d'accès 53
8.4.1 Composants obligatoires spécifiques au profil dans les jetons d'accès 53
8.4.2 Composants facultatifs des jetons d'accès 54
8.4.3 Définition des champs spécifiques 55
8.5 Profils des jetons d'accès 60
8.5.1 Généralités 60
8.5.2 Profil A: Certificat X.509 de clé publique 60
8.5.3 Profil B: Certificat X.509 d'attribut 64
8.5.4 Profil C: Jeton web JSON – JWT 68
8.5.5 Profil D: Informations sur le jeton d'accès fournies par RADIUS 71
8.5.6 Profil E: Informations RBAC fournies par LDAP 74
9 Vérification des jetons d'accès 80
9.1 Généralités 80
9.2 Existence de plusieurs jetons d'accès 80
9.3 Authentification du sujet 80
9.4 Disponibilité du jeton d'accès 81
9.5 Période de validité 81
9.6 Intégrité des jetons d'accès 81
9.7 Émetteur 82
9.8 Role ID 82
9.9 Révision 82
9.10 Zone de responsabilité 82
9.11 Définition du rôle 83
9.12 État de révocation 83
9.13 Opération 83
9.14 Numéro de séquence 83
9.15 Méthodes de révocation 84
9.15.1 Généralités 84
9.15.2 Méthodes prises en charge 84
10 Modèles de distribution des jetons d'accès RBAC 85
10.1 Généralités 85
10.2 Modèle de PUSH 85
10.3 Modèle de PULL 87
11 Interaction avec les services backend pour la distribution des jetons d'accès RBAC 89
11.1 Généralités 89
11.2 Utilisation des services de répertoire avec LDAP 89
11.2.1 Généralités 89
11.2.2 Communication sécurisée 89

11.2.3 Organisation du répertoire LDAP 91
11.3 Utilisation de l'OAuth pour fournir le jeton JWT 92
11.3.1 Généralités 92
11.3.2 Communication sécurisée 93
11.4 Utilisation des services AAA avec RADIUS 93
11.4.1 Généralités 93
11.4.2 Communication sécurisée 94
11.4.3 Configuration d'homologue 95
11.4.4 Organisation du serveur RADIUS 95
11.5 Comparaison de l'interaction avec le backend en fonction du profil RBAC 95
12 Transport des jetons d'accès 97
12.1 Généralités 97
12.2 Transport dans les protocoles Ethernet 97
12.3 Utilisation dans les protocoles non Ethernet 98
12.4 Utilisation dans le contexte du protocole d'application 98
13 Conformité 98
13.1 Généralités 98
13.2 Notation 98
13.3 Mise en correspondance avec les mécanismes existants d'autorisation 99
13.4 Conformité au format de jetons d'accès 99
13.5 Conformité au contenu des jetons d'accès 99
13.6 Distribution des jetons d'accès 101
13.7 Informations sur les rôles 101
13.8 Échange d'informations relatives au rôle 102
13.9 Événements de sécurité 102
Annexe A (informative) Événements de sécurité 103
A.1 Généralités 103
A.2 Mise en correspondance des événements de sécurité des jetons d'accès généraux 103
A.3 Mise en correspondance des événements de sécurité des jetons d'accès spécifiques aux profils A, B et C 104
A.4 Mise en correspondance des événements de sécurité liés à l'interaction avec le service backend 104
A.5 Mise en correspondance des événements de sécurité liés à l'ingénierie et à la maintenance de RBAC 105
Annexe B (informative) Définition des rôles dans les révisions/éditions précédentes de l'IEC 62351-8 107
B.1 Généralités 107
B.2 Définition des rôles selon l'IEC TS 62351-8:2011 107
B.3 Définition des rôles selon l'IEC 62351-8:2020 108
Annexe C (informative) Exemple informatif de définition de rôle spécifique 110
C.1 Généralités 110
C.2 Description de cas d'utilisation 110
C.3 Exemple de définition XACML 110
C.4 Description du rôle 111
C.5 Description du groupe de permissions 112
C.6 Description de permission 113
C.7 Syntaxe de demande pour le PDP 117
Annexe D (informative) Exemples d'interaction LDAP 118

D.1 Généralités 118
D.2 Import du nouveau schéma LDAP pour "IEC6351-RoleStructure" 118
D.3 Import du nouveau schéma LDAP pour "roles" 118
Annexe E (informative) Application générale de jetons d'accès RBAC 119
E.1 Généralités 119
E.2 Approche par session 119
E.3 Approche par message 121
Bibliographie 122

Figure 1 – Cadre générique du contrôle d'accès 21
Figure 2 – Schéma de RBAC avec séparations statique et dynamique des responsabilités (version améliorée de l'ANSI INCITS 359-2004) 22
Figure 3 – Vue d'ensemble sur les concepts de sujets, rôles, permissions et `operationSets` 25
Figure 4 – Documents de référence 30
Figure 5 – Relation entre les rôles et les permissions 31
Figure 6 – Liaison d'objets à l'aide de fichiers de rôles et de permissions distincts 34
Figure 7 – Structure XACML 35
Figure 8 – Liaison d'objets à l'aide d'`operationSets` et de fichiers O2OS 40
Figure 9 – Définition des `operationSets` sur l'exemple de l'IEC 61850 42
Figure 10 – Affectation des `operationSets` aux objets qui utilisent des fichiers O2OS 43
Figure 11 – Rôles génériques – Corrélation des documents de référence avec l'IEC 62351-8 avec des exemples de triplets d'identification de rôle 47
Figure 12 – Exemple d'arborescence LDAP 77
Figure 13 – Rôles de classe d'objets LDAP 77
Figure 14 – Affectation des groupes LDAP à des rôles connus d'IED 78
Figure 15 – Affectation LDAP memberOf 79
Figure 16 – Vue schématique de l'autorisation d'après le modèle PUSH de RBAC 86
Figure 17 – Vue schématique de l'autorisation d'après le modèle PULL de RBAC 88
Figure 18 – Modèle RBAC avec flux de travail OAuth appliquant JWT 92
Figure E.1 – Approche RBAC par session (sécurité de bout en bout de l'IEC 62351-4 simplifiée) 121

Tableau 1 – Versions publiées et nom d'espace de nom associé 13
Tableau 2 – Attributs de l'élément de code de l'IEC 62351-8 13
Tableau 3 – Rôles prédéfinis 28
Tableau 4 – Modèle de mise en correspondance rôle-permission 32
Tableau 5 – Modèle de définition des permissions 32
Tableau 6 – Contexte d'évaluation 40
Tableau 7 – Plage possible de permissions par rôle 42
Tableau 8 – Mise en correspondance des événements de sécurité selon l'IEC 62351-14 45
Tableau 9 – Jeton d'accès: métadonnées d'informations 53
Tableau 10 – Jeton d'accès: informations sur le rôle de l'utilisateur 54
Tableau 11 – Composants facultatifs des jetons d'accès 54

Tableau 12 – Champs et format de l'AoR 59
Tableau 13 – Exemple informatif: Gestion de l'AoR sur un IED 60
Tableau 14 – Mise en correspondance entre ID et certificat d'attribut 68
Tableau 15 – Comparaison des profils RBAC 96
Tableau 16 – Conformité au format de jetons d'accès 99
Tableau 17 – Jeton d'accès: métadonnées d'informations 100
Tableau 18 – Jeton d'accès: informations sur le rôle de l'utilisateur 100
Tableau 19 – Composants facultatifs des jetons d'accès 100
Tableau 20 – Prise en charge des rôles génériques 101
Tableau 21 – Conformité à la distribution des jetons d'accès 101
Tableau 22 – Prise en charge des rôles prédéfinis 102
Tableau A.1 – Événements de sécurité des jetons d'accès généraux mis en correspondance selon l'IEC 62351-14 103
Tableau A.2 – Événements de sécurité des jetons d'accès spécifiques des profils A, B et C mis en correspondance selon l'IEC 62351-14 104
Tableau A.3 – Journaux des événements de sécurité liés à l'interaction avec le service backend 104
Tableau A.4 – Journaux des événements de sécurité liés à l'ingénierie et à la maintenance de RBAC 105
Tableau B.1 – Liste d'affectations rôle-permission prédéfinies (version 2011) 107
Tableau B.2 – Liste d'affectations rôle-permission prédéfinies (version 2021) 108
Tableau C.1 – Affectation de permission 110

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.

Les éléments de code associés sont des fichiers d'exemple XACML pour la définition de rôles personnalisés. Seule une version complète est disponible. Elle est librement accessible pour téléchargement sur le site web de l'IEC à l'adresse suivante: http://www.iec.ch/tc57/supportdocuments. Son utilisation reste cependant soumise aux conditions de licence.

En cas de divergence entre l'élément de code téléchargeable et le contenu pdf publié par l'IEC, l'élément de code téléchargeable prévaut. Il peut faire l'objet de mises à jour. Voir l'historique des fichiers inclus.

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).

IEC TS 62351-2, *Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms* (disponible en anglais seulement)

IEC 62351-3:2023, *Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 3: Sécurité des réseaux et des systèmes de communication - Profils comprenant TCP/IP*

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks* (disponible en anglais seulement)

Registre des numéros d'entreprise privée de l'IANA: https://www.iana.org/assignments/enterprise-numbers/

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

IETF RFC 4513, *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms* (disponible en anglais seulement)

IETF RFC 6614, *Transport Layer Security (TLS) Encryption for RADIUS* (disponible en anglais seulement)

IETF RFC 6749, *The OAuth 2.0 Authorization Framework* (disponible en anglais seulement)

IETF RFC 7519, *JSON Web Token (JWT)* (disponible en anglais seulement)

XACML-RBAC, *XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0, October 2014*. Disponible à l'adresse: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-rbac-v1-spec-en.html

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC TS 62351-2 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:

– IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

– ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
jeton d'accès
preuve ou témoignage concernant les droits de chacun au crédit, à la confiance ou à l'autorité

3.2
zone de responsabilité
zone (géographique ou organisationnelle) dans laquelle le rôle est applicable

3.3
agent automatisé
programme informatique fonctionnant sur une seule machine, qui effectue des opérations locales et/ou distantes indépendamment des entrées utilisateur

3.4
Séparation Dynamique des Responsabilités
DSD
limitation de la disponibilité des permissions par le biais de contraintes sur les rôles pouvant être activés pendant une session utilisateur ou entre deux sessions utilisateur

Note 1 à l'article: La séparation dynamique des responsabilités fournit la capacité à traiter d'éventuelles questions de conflit d'intérêts lorsque l'utilisateur se voit affecté à un rôle. La séparation dynamique des responsabilités permet l'autorisation d'un utilisateur à des rôles ne donnant pas lieu à des conflits d'intérêts lorsqu'ils agissent de manière indépendante, mais qui donnent lieu à des préoccupations relatives aux politiques lorsqu'ils sont activés de manière simultanée. Bien que cette séparation de responsabilités puisse être possible par l'établissement d'une relation de séparation statique des responsabilités, les relations de séparation dynamique des responsabilités améliorent généralement la souplesse opérationnelle de l'entreprise.

Note 2 à l'article: L'abréviation "DSD" est dérivée du terme anglais développé correspondant "dynamic separation of duty".

3.5
entité
toute instance configurée avec des affectations rôle-permission, s'appuyant sur les jetons d'accès

3.6
détenteur
utilisateur qui possède ou détient un jeton d'accès lié à un certificat de clé publique ou à une entité nommée

[SOURCE: IETF RFC 5755]

3.7
fournisseur d'identité
instance qui crée, maintient et gère les informations relatives à l'identité, généralement utilisée dans les scénarios d'authentification unique