IEC 62351-8

Edition 1.0 2020-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-8072-0

CONTENTS

Document history

Any person intervening in the present document is invited to complete the table below before sending the document elsewhere. The purpose is to allow all actors to see all changes introduced and the intervening persons.

Any important message to IEC editors should also be included in the table below.

Name of intervening person	Document received		Brief description of the changes introduced	Document sent	
	From	Date		To	Date
Steffen Fries	WG15	2017-03-01	Initial Version		
Steffen Fries	WG15	2017-05-30	Enhancement of OID, More details regarding the RADIUS profile. Clarification of relationship to PULL and PUSH models, which led to a re-write of the current describtion focussing solely on LDAP		
Steffen Fries	WG15	2017-07-28	Enhancement of the area of responsibility section. Standard of profile specific parameters in the access token.		
Frances Cleveland	Steffen Fries	2017-08-31	Editorial updates		2017-9-22
Steffen Fries	Frances Clevela nd	2017-09-22	Further Updates of the RADIUS profile with an index option to allow for multiple roles per user ith different AoR or Revision Deperecation of Profile C		
Steffen Fries		2017-11-22	Further description of Profile D and application itegration examples. Deletion of exisiting Profile C		
Steffen Fries		2018-02-22	Update on RADIUS, Inclusion of custom based role definition		
Steffen Fries		2018-04-30	Refinement of custom based role definition using XACML as proposed in IEC 62351-90-1		
Steffen Fries		2018-06-22	Aligned terminology of rights and permissions throughout the document, refinement of mandatory permissions, inclusion of JWT (based on the contribution of Arijit Bose) as Profile C. Introduction of security events (incidents and warnings) supporting IEC 62351-14.		
Martina Braun	Steffen Fries	2018-06-28	CD doc for circulation	CO	2018-06-28
Steffen Fries		2018-11-28	Incorporation of comment resolution (57/2056/CC) after WG15 meeting in 10/2018	WG15	2018-11-23
Steffen Fries		2018-01-17	Incorporation of final discussion of open issues after WG15 meeting in 01/2019	WG15	
Martina Braun	IEC	2019-05-17	Edited CDV to Project leader for next step	Steffen Fries	2019-05-20
Steffen Fries		2019-05-17	Incorporation of comment resolution for CDV after final discussion wuring web meeting in WG15 on July 1th, 2019 and discussion with IETF RADEST WG (alignment of port number assignment)	IEC	
Martina Braun	Steffen Fries	2019-08-16	FDIS document upload to IEC for circulation	IEC CO	2019-0-23

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE - DATA AND COMMUNICATIONS SECURITY –

Part 8: Role-based access control for power system management

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62351-8 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this standard is based on the following documents:

Enquiry draft	Report on voting
57/2180/FDIS	57/2197/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

This document includes code components i.e components that are intended to be directlyprocessed by a computer. Such content is any text found between the markers <CODE BEGINS> and <CODE ENDS>, or otherwise is clearly labeled in this standard as a code component.

The purchase of this document carries a copyright license for the purchaser to sell software containing code components from this document directly to end users and to end users via distributors, subject to IEC software licensing conditions, which can be found at: http://www.iec.ch/CCv1.

In the case of any discrepancy between the document and the code components, the code components take precedence.

In this document, the following print types are used:

Encoding in ASN.1 or XACML: `couriernew`

A list of all the parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This document provides a standard for access control in power systems. The power system environment supported by this document is enterprise-wide and extends beyond traditional borders to include external providers, suppliers, and other energy partners. Driving factors are the liberalization of the energy sector to include many more stakeholders, the increasingly decentralized generation of energy, and the need to control access to sensitive data of resources and stakeholders. This document supports a distributed security environment in which security is also a distributed service.

The power system sector is continually improving the delivery of energy by leveraging technical advances in computer-based applications. Utility operators, energy brokers and end-users are increasingly accessing multiple applications to deliver, transmit and consume energy in a personalized way. These disparate applications are naturally connected to a common network infrastructure that typically supports protection equipment, substation automation protocols, inter-station protocols, remote access and business-to-business services. Consequently, secure access to these distributed and often loosely coupled applications is even more important than access to an application running on a stand-alone device.

Secure access to computer-based applications involves authentication of the user to the application. After authentication, the types of interactions which that user can perform with the application is then determined. The use of local mechanisms for authorization creates a patchwork of approaches difficult to uniformly administer across the breadth of a power system enterprise. Each application decides with its own logic the authorization process. However, if applications can use a network to help manage access, a database can serve as a trusted source of user’s group or role affiliation. Thus, the access to a shared user base can be controlled centrally. Each application can then examine the permissions listed for a subject and corresponding role and determine their level of authorization.

This document defines role-based access control (RBAC) for enterprise-wide use in power systems. It supports a distributed or service-oriented architecture where security is a distributed service and applications are consumers of distributed services.

In this document, the role of a user is transported in a container called an "access token" of that user to the object. Access tokens are created and administered by a (possibly federated) identity management tool. All access tokens have a lifetime and are subject to expiration. Prior to verification of the access token itself, the user transmitting the access token is authenticated by the object. The object trusts the management tool to issue access tokens with suitable lifetime. This enables local verification of the access token’s validity at remote sites without the need to access a centralized repository (e.g. a centralized revocation list).

Four different access token formats are supported as four different profiles. Two of them are based on X.509 certificates and were already defined in IEC TS 62351-8. Two new profiles are defined as part of this document. The first new profile uses the JSON to encode the access token and the second new profile uses a vendor specific attribute in RADIUS to provide a migration option for environments already utilizing a RADIUS server to support access control. These access tokens may be bound to a specific transport or to a specific application. Common to all access token formats is the information contained, to allow a migration from one profile to another.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE - DATA AND COMMUNICATIONS SECURITY –

Part 8: Role-based access control for power system management

1 Scope

The scope of this part of IEC 62351 is to facilitate role-based access control (RBAC) for power system management. RBAC assigns human users, automated systems, and software applications (collectively called "subjects" in this document) to specified "roles", and restricts their access to only those resources, which the security policies identify as necessary for their roles.

As electric power systems become more automated and cyber security concerns become more prominent, it is becoming increasingly critical to ensure that access to data (read, write, control, etc.) is restricted. As in many aspects of security, RBAC is not just a technology; it is a way of running a business. RBAC is not a new concept; in fact, it is used by many operating systems to control access to system resources. Specifically, RBAC provides an alternative to the all-or-nothing super-user model in which all subjects have access to all data, including control commands.

RBAC is a primary method to meet the security principle of least privilege, which states that no subject should be authorized more permissions than necessary for performing that subject's task. With RBAC, authorization is separated from authentication. RBAC enables an organization to subdivide super-user capabilities and package them into special user accounts termed roles for assignment to specific individuals according to their associated duties. This subdivision enables security policies to determine who or what systems are permitted access to which data in other systems. RBAC provides thus a means of reallocating system controls as defined by the organization policy. In particular, RBAC can protect sensitive system operations from inadvertent (or deliberate) actions by unauthorized users. Clearly RBAC is not confined to human users though; it applies equally well to automated systems and software applications, i.e., software parts operating independent of user interactions.

The following interactions are in scope:

– local (direct wired) access to the object by a human user, a local and automated computer agent, or a built-in HMI or panel;
– remote (via dial-up or wireless media) access to the object by a human user;
– remote (via dial-up or wireless media) access to the object by a remote automated computer agent, e.g. another object at another substation, a distributed energy resource at an end-user's facility, or a control centre application.

While this document defines a set of mandatory roles to be supported, the exchange format for defined specific or custom roles is also in scope of this document.

Out of scope for this document are all topics which are not directly related to the definition of roles and access tokens for local and remote access, especially administrative or organizational tasks, such as:

– user names and password definitions/policies;
– management of keys and/or key exchange;
– engineering process of roles;
– assignment of roles;
– selection of trusted certificate authorities issuing credentials (access tokens);

– defining the tasks of a security officer;

– integrating local policies in RBAC;

NOTE Specifically, the management of certificates is addressed in IEC 62351-9.

Existing standards (see ANSI INCITS 359-2004, IEC 62443 (all parts), and IEEE 802.1X-2004) in process control industry and access control (RFC 2904 and RFC 2905) are not sufficient as none of them specify neither the exact role name and associated permissions nor the format of the access tokens nor the detailed mechanism by which access tokens are transferred to and authenticated by the target system – all this information is needed though for interoperability.

On the other hand, IEEE 1686 already defines a minimum number of roles to be supported as well as permissions, which are to be addressed by the roles. Note that IEEE 1686 is currently being revised.

Throughout the document security events are defined as warnings and alarms. These security events are intended to support the error handling and thus to increase system resilience. It is important implementations provide a mechanism for announcing security events.

Note that for the processing of security warnings and alarms resulting from security logging events and monitoring information there exists separate documents specifying the handling. More specifically, security event handling is specified in IEC 62351-14[1] while the handling of monitoring objects is specified by IEC 62351-7.

Note that warnings and alarms are used to indicate the severity of an event from a security point of view. The following notions are used:

– a warning is intended to raise awareness but to indicate that it may be safe to proceed;

– an alarm is an indication to not proceed.

In any case, it is expected that an operator's security policy determines the final handling based on the operational environment.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850-7-2, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
IEC 62351-3:2014/AMD2:2019[2]

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

---

1 Under preparation. Stage at the time of publication: IEC/CD 62351-14:2019.

2 Under preparation. Stage at the time of publication: IEC BPUB 62351-3/AMD2:2019.

IEC TS 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

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

RFC 5246, *Transport Layer Security (TLS) Protocol version 1.2*

RFC 5288, *AES Galois Counter Mode (GCM) Cipher Suites for TLS)*

RFC 5289, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

RFC 5755, *An Internet Attribute Certificate Profile for Authorization*

RFC 5878, *Transport Layer Security (TLS) Authorization Extensions*

RFC 6749, *The OAuth 2.0 Authorization Framework*

RFC 7519, *JSON Web Token (JWT)*

XACML-RBAC, *XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0, October 2014* [viewed 2019-11-15]. Available at: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-rbac-v1-spec-en.html

SOMMAIRE

Historique du document

Toute personne intervenant sur le présent document est invitée à compléter le tableau ci-dessous avant toute transmission du document. Il s'agit de permettre à tous les acteurs de prendre connaissance de toutes les modifications apportées et de connaître les intervenants correspondants.

Il convient également d'inclure dans le tableau ci-dessous tout message important adressé aux responsables d'édition de l'IEC.

Nom de l'intervenant	Document reçu		Brève description des modifications apportées	Document envoyé	
	De	Date		À	Date
Steffen Fries	WG15	2017-03-01	Version initiale		
Steffen Fries	WG15	2017-05-30	Amélioration de l'OID. Détails supplémentaires concernant le profil RADIUS. Clarification de la relation aux modèles PULL et PUSH, qui a engendré une réécriture de la description actuelle en ciblant exclusivement le LDAP.		
Steffen Fries	WG15	2017-07-28	Amélioration des paragraphes concernant la Zone de responsabilité. Normalisation des paramètres spécifiques aux profils dans le jeton d'accès.		
Frances Cleveland	Steffen Fries	2017-08-31	Mises à jour rédactionnelles		2017-9-22
Steffen Fries	Frances Cleveland	2017-09-22	Mises à jour complémentaires du profil RADIUS avec une option d'indexation permettant l'emploi de plusieurs rôles par utilisateur avec une AoR ou une Revision différente Rejet du Profil C		
Steffen Fries		2017-11-22	Description complémentaire du Profil D et application d'exemples d'intégration. Suppression du Profil C existant.		
Steffen Fries		2018-02-22	Mise à jour du profil RADIUS. Inclusion de la définition de "rôle personnalisé".		
Steffen Fries		2018-04-30	Perfectionnement de la définition de "rôle personnalisé" à l'aide de XACML comme cela est proposé dans l'IEC 62351-90-1.		
Steffen Fries		2018-06-22	Alignement de la terminologie des droits et permissions dans l'ensemble du document, perfectionnement des permissions obligatoires, inclusion du JWT (d'après la contribution d'Arijit Bose) en tant que Profil C. Introduction d'événements de sécurité (incidents et avertissements) prenant en charge l'IEC 62351-14.		
Martina Braun	Steffen Fries	2018-06-28	Projet de comité pour diffusion.	CO	2018-06-28
Steffen Fries		2018-11-28	Intégration de la résolution des commentaires (57/2056/CC) après la réunion du Groupe de travail 15 qui s'est tenue en 10/2018.	WG15	2018-11-23
Steffen Fries		2018-01-17	Intégration du débat final concernant les questions en suspens après la réunion du Groupe de travail 15 qui s'est tenue en 01/2019.	WG15	
Martina Braun	IEC	2019-05-17	CDV rédigé au chef de projet pour l'étape suivante	Steffen Fries	2019-05-20
Steffen Fries		2019-05-17	Intégration de la résolution des commentaires pour le CDV après discussion finale pendant la réunion en ligne du Groupe de travail 15 le 1er juillet 2019 et après discussion avec l'IETF RADEST WG	IEC	
Martina Braun	Steffen Fries	2019-08-16	Mise en ligne du document FDIS à l'IEC pour diffusion	IEC CO	2019-0-23

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'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale 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.

Le texte de cette norme est issu des documents suivants:

Projet d'enquête	Rapport de vote
57/2180/FDIS	57/2197/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation du présent document.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

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 prévus pour être traités directement par un ordinateur. Il s'agit du texte se trouvant entre les marqueurs <CODE BEGINS> et <CODE ENDS>. Sinon, ils sont clairement indiqués dans le présent document comme composants de code.

L'achat de le présent document IEC est accompagné d'une licence de copyright permettant à l'acheteur de vendre des logiciels contenant les composants de code de le 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 – Sécurité des communications et des données*, peut être consultée 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 "http://webstore.iec.ch" dans les données relatives à la publication recherchée. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisé, ou
- amendé.

IMPORTANT – Le logo "*colour inside*" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

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 présent document prend en charge un environnement à sécurité distribuée dans lequel la sécurité est également un service distribué.

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. Elle 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 transporté dans un conteneur, appelé "jeton d'accès", dont fait usage cet utilisateur pour accéder à l'objet. 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 transmet le jeton d'accès est authentifié par l'objet. L'objet fait confiance à l'outil de gestion pour l'émission de jetons d'accès à durée de vie appropriée. Ceci permet la vérification locale de la validité du jeton d'accès à distance sans qu'il soit nécessaire d'accéder à un référentiel centralisé (par exemple, une liste de révocation centralisée).

Quatre formats différents de jetons d'accès sont pris en charge comme quatre profils différents. Deux d'entre eux sont basés sur des certificats X.509 et ont déjà été définis dans l'IEC TS 62351-8. Deux nouveaux profils sont définis dans le cadre du présent document. Le premier profil nouveau utilise JSON pour coder le jeton d'accès et le deuxième profil nouveau utilise un attribut spécifique à un fournisseur dans le profil RADIUS pour fournir une option de migration pour les environnements qui utilisent déjà un serveur RADIUS pour prendre en charge le contrôle d'accès. Ces jetons d'accès peuvent être liés à un transport spécifique ou à une application spécifique. Les informations contenues permettant la migration d'un profil à un autre sont communes à tous les formats de jetons d'accès.

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

1 Domaine d’application

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 du droit d’accès minimal, 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 donne lieu à une organisation permettant de sous-diviser les capacités des super utilisateurs et de les empaqueter dans des rôles de comptes utilisateurs spéciaux destinés à être attribués à des individus spécifiques selon les 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.

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:

– noms d'utilisateur et définitions/stratégies de mot 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-2004) relatives à l'industrie du contrôle de processus et au contrôle d'accès (RFC 2904 et RFC 2905) ne suffisent pas, 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 – néanmoins, toutes ces informations sont nécessaires à des fins d'interopérabilité.

D'autre part, l'IEEE 1686 définit déjà un nombre minimal de rôles à prendre en charge et de permissions que les rôles doivent traiter. À noter que l'IEEE 1686 est en cours de révision.

Dans l'ensemble du document, des événements de sécurité sont définis ainsi que des avertissements et alarmes. 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 important que les mises en œuvre fournissent un mécanisme pour annoncer les événements de sécurité.

À noter que pour le traitement des avertissements et alarmes de sécurité résultant d'événements de connexion de sécurité et d'informations relatives à la surveillance, il existe des documents distincts spécifiant leur gestion. Plus spécifiquement, la gestion des événements de sécurité est spécifiée dans l'IEC 62351-14[1], tandis que la gestion des objets de surveillance est spécifiée dans l'IEC 62351-7.

À noter que les avertissements et les alarmes sont utilisés pour indiquer la sévérité d'un événement du point de vue de la sécurité. Les notions suivantes sont utilisées:

– un avertissement était destiné à susciter une prise de conscience, mais indique également qu'une action peut être effectuée en toute sécurité;
– une alarme indique de ne pas poursuivre.

Il est, en toute circonstance, prévu qu'une politique de sécurité de l'opérateur détermine le traitement final selon l'environnement opérationnel.

2 Références normatives

Les documents suivants cités dans le texte 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).

[1] En cours d'élaboration. Stade au moment de la publication: IEC/CD 62351-14:2019.

IEC 61850-7-2, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*

IEC TC 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)IEC 62351-3:2014, *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*
IEC 62351-3:2014/AMD2:2019[2]

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives* (disponible en anglais seulement)

IEC TS 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control* (disponible en anglais seulement)

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

RFC 5246, *Transport Layer Security (TLS) Protocol version 1.2*

RFC 5288, *AES Galois Counter Mode (GCM) Cipher Suites for TLS)*

RFC 5289, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

RFC 5755, *An Internet Attribute Certificate Profile for Authorization*

RFC 5878, *Transport Layer Security (TLS) Authorization Extensions*

RFC 6749, *The OAuth 2.0 Authorization Framework*

RFC 7519, *JSON Web Token (JWT)*

XACML-RBAC, *XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile* Version 1.0, octobre 2014 [consulté 2019-11-15]. Adresse http://docs.oasis-open.org/xacml/3.0/xacml-3.0-rbac-v1-spec-en.html

[2] En cours d'élaboration. Stade au moment de la publication: IEC BPUB 62351-3/AMD2:2019.