IEC 62351-8

Edition 2.0 2026-07

INTERNATIONAL STANDARD

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

ICS 33.200

ISBN 978-2-8327-1354-9

IEC 62351-8:2026-07(en)

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

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

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

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

This second edition cancels and replaces the first edition published in 2020. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) Removal of mapping of roles to permission to objects based on the target data model and/or protocol to allow for other mappings than IEC 61850. Mapping is delegated to separate documents;
b) Specification of handling of a combination of roles and permissions as operationSet to allow more fine-grained assignments to objects;

c) Specification of a simplified roles assignment to more efficiently handle situations in which roles are used relating to different data models, including examples;

d) Inclusion of new profile to allow for fetching RBAC information from LDAP repositories;

e) Definition of specific security events throughout the document;

f) Alignment of terminology and enhancement with examples.

The text of this International Standard is based on the following documents:

Draft	Report on voting
57/2882/FDIS	57/2921/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

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 directly processed by a computer. Such content is any text found between the markers <CODE BEGINS> and <CODE ENDS>, or otherwise is clearly labelled in this document 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 document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

– reconfirmed,

– withdrawn, or

– revised.

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.

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 that the user can perform with the application is then determined. The use of local mechanisms for authorization creates a patchwork of approaches which are 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 contained in a data structure called "access token" for that user and is provided to the accessed resource. Access tokens are created and administered by a (possibly federated) identity management. All access tokens have a lifetime and are subject to expiration. Prior to verification of the access token itself, the user who tries to get access is authenticated by the resource. The resource has a trust relation to the access token management. The access token can be provided as self-contained object by the user or a central repository or as data structure by a central repository. Specifically, the self-contained access tokens enable local verification of the access token's validity at remote sites without the need to access a centralized repository. To ensure availability of information in the repository, redundancy may be considered. Note that redundancy concepts are out of scope for this document.

Different access token formats are supported as five defined profiles. These access tokens can be bound to a specific transport or to a specific application in conjunction with different types of repositories, holding the access tokens. Common to all profiles is the information contained, to allow a migration from one profile to another.

As RBAC is being adopted for several protocols and data models this document has been changed accordingly. In its current version it focuses on the general definition of RBAC, mandatory to be supported roles and options for assigning roles to permissions. The actual assignment of roles to permissions, and consequently the binding of RBAC related information to objects, is addressed in the referencing documents, which directly relate to the target data model. The existing definition of the IEC 61850 specific roles and permissions has been moved to IEC 61850-90-19. Likewise for IEC 60807-5-101/-104 the specifics are handled in IEC 60870-5-7:2025. Moreover, IEEE 1815 specifics will be handled in the context of DNP3SAv6. This document provides information about the role to permission assignment of previous versions of this document in Annex B.

This standard is maintained. Technical issues identified after publication will be handled via the TISSUE database to keep correctness and interoperability. Approved technical issues will be published as INF document and might be further handled according to IEC directives.

1 Scope

1.1 General

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 thus provides 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 human machine interface (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. This is achieved by defining two different encoding approaches to handle the definition of custom roles, either based on specific permissions or based on constraints to existing permissions. The definition on handling custom based roles was started in IEC 62351-90-1 and taken over into the IEC 62351-8:2020. Moreover, additionally to the definition of custom roles based on associated permissions, this document also includes options how to assign permissions to objects in a general way. Referencing documents will provide a mapping to a concrete data model to ensure an interoperability for standard roles used in different data models as well as for custom defined roles. Referencing documents might be standards such as IEC PAS 61850-90-19 or IEC 60870-5-7:2025 or also definitions by an operator.

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:

– definition of usernames and password definitions/policies;
– management of keys and/or key exchange;
– engineering process of roles;
– assignment of roles;
– selection of trusted certification 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-2020) in process control industry and access control (RFC 2904 and RFC 2905) are not sufficient for addressing specifics of power system automation as none of them specify either the exact role name and associated permissions or the format of the access tokens nor the detailed mechanism by which access tokens are transferred to and authenticated by the target system. This is addressed in this document by defining the access token format, distribution and verification based on existing technology.

Throughout the document security events are defined. These security events are intended to support the error handling and thus to increase system resilience. Implementations need to provide a mechanism for announcing security events.

The information about security events and potential detailed information can only be provided by the entity based on the availability of this information through the underlying platform or utilized components.

It is strongly recommended that the security events defined throughout the document are made available to the operational infrastructure by cyber security events as specified in IEC 62351-14 and/or by monitoring objects as specified in IEC 62351-7. Annex A provides a mapping of the defined events in this document to the notion of IEC 62351-14.

Notices, warnings, errors, and alarms are used to indicate the severity of an event from a security point of view. The following notion from IEC 62351-14 is used:

– A *notice* refers to a cyber security related activity during the routine use or maintenance of an entity. It does not relate to a cyber security breach or attack or deviation from the normal operating condition of an entity.
– A *warning* is a deviation from the normal operating condition of an entity but not necessary a cyber-attack.
– An *error* describes an unforeseen condition, which can indicate unauthorized activity. It might not require immediate action.
– An *alarm* is an indication of a serious problem, which might indicate unauthorized activity. Action is expected to be taken immediately.

In any case, it is expected that an organization’s security policy determines the final handling of events based on the operational environment. For instance, the assessment of one of more alarms could rise to the level of an incident.

1.2 Published versions of the standard and related namespace names

Table 1 provides a reference between all published editions, amendments or corrigenda of this document and the full name of the namespace.

Table 1 – Published versions and related namespace names

Edition	Publication date	Webstore	Namespace
TS Edition 1.0	2011-09	IEC 62351-8:2011	
IS Edition 1.0	2020-04	IEC 62351-8:2020	
IS Edition 2.0	2026-07	IEC 62351-8:2026	

1.3 Identification of the code component

The code components associated with this document are XACML examples in XML files for the definition of custom based roles as well as example LDAP schema as LDIF files as well as the definitions for RBAC access tokens for profile A and B as ASN file and Profile C as JSON file.

The parameters which identify the code components are provided in Table 2:

Table 2 – Attributes of the IEC 62351-8 code component

Attribute	Content
Version	2026
Revision	A
Release	1
Code Component Name	IEC_62351-8.ASN1-JSON-XACML-LDIF-Examples.2026A.full.IS

Note that the code components do not provide an own namespace and rather rely on the XACML namespaces defined in the associated W3C specification.

1.4 Code Component distribution

Each Code Component is a ZIP package containing the electronic representation of the Code Component itself, with a file describing the content of the package (IECManifest.xml).

The life cycle of a code component is not restricted to the life cycle of the related publication. The publication life cycle goes through two stages, Version (corresponding to an edition) and Revision (corresponding to an amendment). A third publication stage (Release) allows publication of Code Component in case of urgent fixes of InterOp Tissues, thus without need to publish an amendment.

Consequently, new releases of the Code Component may be released, which supersedes the previous release, and will be distributed through the IEC TC 57 web site at:

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

The latest version/release of the code component will be found by selecting the file for the code component with the highest value for VersionStateInfo, e.g. IEC_62351-8.ASN1-JSON-XACML-LDIF-Examples.{VersionStateInfo}.full.zip.

The code components associated with this IS are XACML example files for the definition of custom based roles. It is available as a full version only. It is freely accessible on the IEC website for download at https://www.iec.ch/tc57/supportdocuments, but the usage remains under the licensing conditions.

In case of any differences between the downloadable code component and the IEC pdf published content, the downloadable code component is the valid one; it might be subject to updates. See included history files.

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 TS 62351-2, *Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms*

IEC 62351-3:2023, *Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including 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*

IANA Private Enterprise Numbers Registry: 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*

IETF RFC 6614, *Transport Layer Security (TLS) Encryption for RADIUS*

IETF RFC 6749, *The OAuth 2.0 Authorization Framework*

IETF 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*. Available at:
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-rbac-v1-spec-en.html

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

– IEC Electropedia: available at http://www.electropedia.org/
– ISO Online browsing platform: available at http://www.iso.org/obp