SVENSK STANDARD SS-EN IEC 62351-8

Fastställd	Utgåva	Sida	Ansvarig kommitté
2020-11-11	1	1 (1+76)	SEK TK 57

Styrning av kraftsystem och tillhörande informationsutbyte – IT-säkerhet – Del 8: Rollbaserad åtkomst för styrning av kraftsystem

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

Som svensk standard gäller europastandarden EN IEC 62351-8:2020. Den svenska standarden innehåller den officiella engelska språkversionen av EN IEC 62351-8:2020.

Nationellt förord

Europastandarden EN IEC 62351-8:2020

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC
– **IEC 62351-8, First edition, 2020 - Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management**

utarbetad inom International Electrotechnical Commission, IEC.

ICS 33.200.00

Denna standard är fastställd av SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00.
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard
Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62351-8

June 2020

ICS 33.200

English Version

Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management (IEC 62351-8:2020)

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 (IEC 62351-8:2020)

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 8: Rollenbasierte Zugriffskontrolle für Energiemanagementsysteme (IEC 62351-8:2020)

This European Standard was approved by CENELEC on 2020-06-02. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN IEC 62351-8:2020 E

European foreword

The text of document 57/2180/FDIS, future edition 1 of IEC 62351-8, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62351-8:2020.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2021-03-02
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-06-02

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62351-8:2020 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60870-5-104	NOTE	Harmonized as EN 60870-5-104
IEC 61784 (series)	NOTE	Harmonized as EN IEC 61784 (series)
IEC 61850-8-1	NOTE	Harmonized as EN 61850-8-1
IEC 61850-8-2	NOTE	Harmonized as EN IEC 61850-8-2
IEC 61968 (series)	NOTE	Harmonized as EN 61968 (series)
IEC 61970 (series)	NOTE	Harmonized as EN 61970 (series)
IEC 62351-7:2017	NOTE	Harmonized as EN 62351-7:2017 (not modified)
IEC 62351-9	NOTE	Harmonized as EN 62351-9
IEC 62351-14	NOTE	Harmonized as EN IEC 62351-14[1]
IEC 62443 (series)	NOTE	Harmonized as EN IEC 62443 (series)

[1] To be published. Stage at the time of publication: prEN IEC 62351-14:2019.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
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)	EN 61850-7-2	-
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	EN 62351-3	2014
+ A2	2020		+ A2	2020
IEC 62351-4	-	Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS and derivatives	EN IEC 62351-4	-
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	-	The 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	2014	XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0, October 2014.	-	-

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