IEC/TS 62351-8

Edition 1.0 2011-09

TECHNICAL SPECIFICATION

colour inside

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

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

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 corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TS 62351-8

Edition 1.0 2011-09

TECHNICAL SPECIFICATION

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-88912-723-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 8: Role-based access control

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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-8, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/1119/DTS	57/1153/RVC

Full information on the voting for the approval of this technical specification 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.

A list of all the parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security,* 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

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

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 Technical specification covers access control in power systems. The power system environment supported by this specification 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, the increasingly decentralized generation of energy, and the need to control access to data of precious resources. This specification 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 object.

Secure access to computer-based applications involves authentication of the user to the application. After authentication, the level at which a user can use the application is 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 the authorization on its own logic. If applications can use a network, 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 rights listed for a subject and corresponding role and determine their level of authorization.

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 must be 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).

Three different access token formats are supported as three different profiles. Two of them are X.509 Access tokens and the third is a software token similar to Kerberos. They can be used over TCP/IP and serial communication links.

This specification 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.

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

Part 8: Role-based access control

1 Scope

This technical specification covers the access control of users and automated agents – in the following subjects – to data objects in power systems by means of role-based access control (RBAC). RBAC is not a new concept used by many operating systems to control access to system resources. RBAC is an alternative to the all-or-nothing super-user model. RBAC is in keeping with the security principle of least privilege, which states that no subject should be given more rights than necessary for performing that subject's job. RBAC enables an organization to separate super-user capabilities and package them into special user accounts termed roles for assignment to specific individuals according to their job needs. This enables a variety of security policies, networking, firewall, back-ups, and system operation. A site that prefers a single strong administrator but wants to let more sophisticated users fix portions of their own system can set up an advanced-user role. RBAC is not confined to users however, it applies equally well to automated computer agents, i.e., software parts operating independent of user interactions. The following interactions are covered by the scope of this technical specification:

– local (direct wired) access to the object by a human user;
– local (direct wired) access to the object by a local and automated computer agent, e.g. another object at the substation;
– direct access by a user to the object using the objects' 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, or a control centre application.

As in many aspects of security, RBAC is not just a technology; it is a way of running a business. As subject names change more frequently than role names and as role names change more frequently than the rights of a data model (e.g. IEC 61850), it is advisable to store the frequently changing entities (i.e. the subjects names) outside the object. Less frequently changing role names and rights are stored inside the object.

RBAC thus provides a means of reallocating system controls as defined by the organization policy.

The scope of this specification covers everything that is needed for interoperability between systems from different vendors. The purpose of this specification is therefore:

– firstly, to introduce 'subjects-roles-rights' as authorization concept;
– secondly, to promote role-based access control for the entire pyramid in power system management; and
– thirdly, to enable interoperability in the multi-vendor environment of substation automation and beyond.

Out of scope for this specification 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 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 These issues will be addressed in IEC/TS 62351-9[1].

The IEC 62351 series specifies end-to-end security in power systems so that secure connections are established between applications. RBAC is recognized as a potentially efficient and safe means to control access to data objects.

Existing standards (see [ANSI INCITS 359-2004], [IEC 62443], and [IEEE 802.1X-2004]) in the process control industry and access control ([RFC2904] and [RFC2905]) are not sufficient as none of them specify either the exact role name and associated rights, the format of the access tokens or the detailed mechanism by which access tokens are transferred to and authenticated by the target system – however, all this information is needed though for interoperability.

2 Normative references

The following referenced documents are indispensable for the application 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 (all parts), *Communication networks and systems in substations*

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 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC/TS 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

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

IEC/TS 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

ISO 9594-8/ITU-T Recomendation X.509:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

[1] Under consideration.

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions of IEC/TS 62351-1 apply, as well as the following.

3.1 Terms and definitions

3.1.1
area of responsibility
range of authority, for instance based on network segregation

3.1.2
automated agent
computer program running on a single machine

NOTE It performs local and/or remote operations independent of user inputs

3.1.3
access token
evidence or testimonials concerning one's right to credit, confidence, or authority

3.1.4
holder
entity that possesses or owns an access token

3.1.5
issuer
entity that issues an access token

3.1.6
identity provider
entity that creates, maintains and manages identity information; typically used in single sign-on scenarios

3.1.7
object
any system resource subject to access control such as a file, printer, terminal, database record, etc.

3.1.8
operation
executable image of a program which upon invocation executes some function/activity for the subject

3.1.9
privilege
attribute or property assigned to a subject by an authority

3.1.10
privilege management infrastructure
PMI
the infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a public key infrastructure

3.1.11
right
atomic set of accessing privileges assigned to a particular system object

3.1.12
role
job function within the context of an organization with some semantics associated regarding the authority and responsibility conferred on the user assigned to the role

NOTE A role subsumes a set of rights.

Pre-defined role: a role that is defined in this specification.

Default role: a role that is defined by the vendor of the protection equipment (not by its specification) and that is valid generally for all objects of that vendor.

Specific role: a role that is defined by the utility operator for its particular needs.

3.1.13
service
permission in the context of IEC 61850

3.1.14
session
encounter between a user and an application or with the computer in general

NOTE One user session is the time between starting the communication channel (either local or remote) and terminating (either by the user or the system).

3.1.15
static separation of duty
SSD
enforcement constraints on the assignment of users to roles

NOTE Membership in one role may prevent the user from being a member of one or more other roles, depending on the SSD rules enforced.

3.1.16
dynamic separation of duty
DSD
limitation of the availability of rights by placing constraints on the roles that can be activated within or across a user's sessions

NOTE 1 DSD provides the capability to address potential conflict of interest issues at the time a user is assigned to a role.

NOTE 2 DSD allows a user to be authorized for roles that do not cause a conflict of interest when acted in independently, but which produce policy concerns when activated simultaneously. Although this separation of duty could be achieved through the establishment of a static separation of duty relationship, DSD relationships generally provide the enterprise with greater operational flexibility.

3.1.17
out-of-band
communications which occur outside a previously established communication method or channel

3.1.18
service provider
an object that provides services

NOTE It is subject to access control.

3.1.19
subject
user or an automated agent

NOTE A subject is a right holder. It has a name attribute whose value is mandatory. It is this name that is used to enrol a subject in a particular role.