IEC TR 62351-90-1

Edition 1.0 2018-01

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 90-1: Guidelines for handling role-based access control in power systems

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-5233-8

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 90-1: Guidelines for handling role-based access control in power systems

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. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 62351-90-1, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This publication contains attached files in the form of electronic machine readable files. These files are intended to be used as a complement and do not form an integral part of the publication.

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

Enquiry draft	Report on voting
57/1905/DTR	57/1942/RVDTR

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

This document 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.

This IEC Technical Report 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 labeled in this standard as a Code Component.

The purchase of this IEC standard carries a copyright license for the purchaser to sell software containing Code Components from this standard 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.

The Code Components included in this IEC standard are also available as electronic machine readable files at: http: //www.iec.ch/public/TC57/IEC_62351-90-1.XACML-Examples.full.TR.zip.

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

- 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

The power system sector is adopting security measures to ensure the reliable delivery of energy. One of these measures comprises Role-based Access Control (RBAC), allowing utility operators, energy brokers and end-users to utilize roles to restrict the access to equipment and energy automation functionalities on a need-to-handle basis. The specific measures to realize this functionality have been defined in the context of IEC TS 62351-8. It defines three profiles for the transmission of RBAC related information. This information includes, but not limited to, being contained in public key certificates, attribute certificates, or software tokens. Moreover, especially for IEC 61850, it defines a set of mandatory roles and associated rights. IEC 61850 also allows the definition of custom roles and associated rights, but this is not specified in a way to ensure interoperability.

Implementations of RBAC have shown that utilities are likely to have their own set of roles and associated rights that need to be supported. Therefore, this technical report enhances the solution for role based access control in power systems defined in IEC TS 62351-8. It provides best practice guidelines for the distribution of role-to-right information targeting the definition of custom roles besides the mandatory roles defined in IEC TS 62351-8. As defined in IEC TS 62351-8, roles of a user are transported in a container called an access token. Access tokens are assumed to be created and administered by an identity management tool. IEC TS 62351-8 currently defines three different formats for such access tokens.

This technical report targets the provisioning of guidance for the implementation of RBAC. More specifically it focuses on means to describe custom roles, as well as the management of these new roles and associated rights, which are typically administered in a management tool and enforced in the endpoints. By defining categories, the workflow is simplified for defining new roles and associated rights besides the predefined roles in IEC TS 62351-8 as well as the assignment to subjects. Consequently the information exchange necessary to distribute the RBAC information is also a target of this technical report to ensure interoperability between different vendor’s products. This is achieved by utilizing the existing standard XACML. In addition to IEC TS 62351-8 further constraints of role execution are considered. These constraints are bound to the execution environment rather than the access token carrying the role information itself.

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

Part 90-1: Guidelines for handling role-based access control in power systems

1 Scope

This part of IEC 62351, which is a technical report, addresses the handling of access control of users and automated agents to data objects in power systems by means of role-based access control (RBAC) as defined in IEC TS 62351-8. IEC TS 62351-8 defines three different profiles to distribute role information and also defines a set of mandatory roles to be supported. Adoption of RBAC has shown that the defined mandatory roles are not always sufficient and it is recommended that the method for defining custom roles be standardized to ensure interoperability. Hence, the main focus of this document lies in developing a standardized method for defining and engineering custom roles, their role-to-right mappings and the corresponding infrastructure support needed to utilize these custom roles in power systems. This is achieved by defining categories and sub level categories, which provide a distinction of actions, connected with dedicated rights as well as a proposal for a format to distribute the custom role-to-right mappings. Moreover, a format is being proposed to distribute the information on custom defined roles and associated rights by utilizing XACML as an established standard for access control.

Besides the discussion of handling custom roles, this document also addresses the following issues:

– Providing recommendations and/or examples for role-right-operation and (object) association to ensure interoperability from operational and developers point of view.

– Providing mechanisms and rules to avoid overloading of existing roles by allowing for an aligned way to define new (custom) roles.

– Easing the administration of roles in IEDs from a device management point of view:

  - Allowing for centralized assignment of roles, by maintaining the same associations on device/application level.
  - Avoiding the definition of role-right-operation on command level to cope with diverse application environment of IEC TS 62351-8 (e.g. IED, substation level, control centre, SCADA).

– Enhancing available constraints for acting in a specific role considering the local environment with respect to operational constraints.

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 61850-6, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

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 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 TS 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

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

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

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

OASIS XACML eXtensible Access Control Markup Language, Version 3