DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 29146

ISO/IEC JTC **1**/SC **27** Secretariat: **DIN**

Voting begins on: **2015-07-27** Voting terminates on: **2015-10-27**

Information technology - Security techniques - A framework for access management

Technologies de l'information — Techniques de sécurité — Cadre pour gestion d'accès

ICS: 35.040

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 29146:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents Page

Figures

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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

ISO/IEC 29146 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information technology Subcommittee*.

Introduction

Management of information security is a complex task that is based primarily on risk-based approach, and that is supported by several security techniques. The complexity is handled by several supporting systems that can automatically apply a set of rules or policies consistently.

Within the management of information security, access management plays a key role in the administration of the relationships between the accessing party (subjects that can be human or non-human entities) and the information technology resources. With the development of the Internet, information technology resources can be located over distributed networks, and the access to them needs to be managed in conformity under a policyand is expected to have common terms and models as a framework on access management.

Within the management of information security, identity management also plays a key role. Access management is mediated through the identification and authentication of subjects that seek to access information technology resources. This standard depends on the existence of an underlying identity management system or identity management infrastructure. Regarding this topic, see references in normative references section.

This framework for access control is one part of an overall Identity and access management framework. The other part is the framework for identity management, which is defined in ISO/IEC 24760.

This framework describes the concepts, actors, components, reference architecture, functional requirements and practices for access control. Example access control models are included.

It focuses mainly on access control for a single organization, but adds other considerations for access control in collaborative arrangements across multiple organizations.

Information technology — Security techniques — A framework for access management

1 Scope

This International Standard defines and establishes a framework for Access Management (AM) and the secure management of the process to access information and Information and Communications Technologies ICT information resources, associated with the accountability of a subject within some context.

This International Standard provides concepts, terms and definitions applicable to distributed access management techniques in network environments.

This International Standard also provides explanations about related architecture, components and management functions.

The subjects involved in access management might be uniquely recognized to access information systems, as defined in ISO/IEC 24760,"A framework for identity management".

The nature and qualities of physical access control involved in access management systems are outside the scope of this document.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applied. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ISO/IEC 24760-1, *Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts.*
- ISO/IEC 24760-2, *Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements.*
- ISO/IEC 24760-3,† *Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice.*
- ISO/IEC 29115, *Information technology -- Security techniques -- Entity authentication assurance framework.*
- ISO/IEC 27002, *Information technology -- Security techniques -- Code of practice for information security controls.*

† to be published

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24760-1 and ISO/IEC 29115, as well as the following apply.

3.1
access control
process of granting or denying an operation to be performed on a resource (3.14) by a subject and of auditing the decision in an audit trail.

NOTE 1 A primary purpose of access control is to prevent unauthorized access to information or use of ICT resources based on the business and security requirements; that is, the application of authorization policies to particular access requests.

NOTE 2 When an authenticated subject makes a request, the resource owner will authorize (or not) access in accordance with access policy and subject privileges.

3.2
access management
set of processes to manage access control (3.1) for a set of resources (3.14)

3.3
access token
result of access authorization decision

3.4
attribute
characteristic or property used to describe and to control access to a resource

NOTE 1 The rules for accessing a resource are defined in an access control policy which specifies the attributes required for the granting of access by a subject to a resource for a specific operation

NOTE 2 Attributes can include subject attributes, resource attributes, environmental attributes and other attributes used to control access as specified in the access control

3.5
endpoint
location in an access management system where an access control function is performed

NOTE 1 There can be different types of endpoints:
- authentication endpoint, where subject authentication is performed
- authorization endpoint, where subject authorization is performed
- resource endpoint, where access control for a resource is applied
- endpoint discovery service, that searches for and locates endpoints.
- initial endpoint discovery service, used at the start of subject interactions with an access management system

NOTE 2 Endpoint discovery services are commonly used in distributed and networked systems.

3.6
Enterprise implementation
Implementation pattern of AMS as services where PEP plays the crucial role

3.7
need-to-know
security objective of keeping the subject's access to data resources to the minimum necessary for a requesting user to perform their functions

NOTE 1 Need-to-know is authorized at the discretion of the resource owner

NOTE 2 Need-to-have is the security objective of the requester for the fulfilment of specific tasks that may be limited at the resource owner’s discretion

3.8
privilege
access right
permission
assignment to a particular subject of the right to access data

NOTE 1 Privilege is necessary but not sufficient condition for access. Access occurs when the access request is granted according to its access control policy. The access control policy is based on privileges and may include other environmental factors (e.g. time-of-day, location etc.)

NOTE 2 Data presented by a subject or obtained for a subject which is used by a Policy Decision Point in order to grant or deny an operation that a subject is willing to perform on a resource.

NOTE 3 A resource may have multiple distinct privileges associated with it which correspond to various defined levels of access. For example, a data resource could have read, write, execute and delete privileges available for assignment to subjects. A request by a subject for access to the resource might be allowed for some levels of access request but disallowed for other levels depending on the level of access requested and the resource privileges that have been assigned to the subject.

3.9
role
name given to a defined set of system functions that may be performed by multiple entities.

NOTE 1 The name is usually descriptive of the functionality

NOTE 2 Entities can be but are not necessarily human subjects

NOTE 3 Roles are implemented by a set of privilege attributes to provide the necessary access to data resources or objects

NOTE 4 Subjects assigned to a role inherit the access privileges associated with the role. In operational use subjects will need to be authenticated as members of the role group before being allowed to perform the functions of the role.

3.10
policy decision point
service that evaluates an access control policy before authorizing access

NOTE 1 When a subject is willing to perform an operation on a resource the PDP is called upon and determines whether the privileges presented by the subject or obtained for the subject allow to grant or deny the requested operation on the resource.

NOTE 2 PDP also audits the decisions in an audit trail and is able to trigger alarms.

NOTE 3 The term corresponds to "Access Decision Function" (ADF) in [ISO10181-3]. It is presumed that this function is located over a network from the subject, and may be located over a network from the corresponding PEP.

3.11
policy enforcement point
service that enforces the access decision by the PDP

NOTE 1 PEP collects the privileges presented by a subject and delivers the information to a PDP for access decision.

NOTE 2 PEP identifies the type of operation to be performed on a given resource and transmits this information to the PDP for the later to apply authorization decisions.

NOTE 3 The term corresponds to "Access Enforcement Function" (AEF) in [ISO10181-3] It is presumed that this function is located over a network from the subject, and may be located over a network from the corresponding PDP.

3.12
policy administration point
service that manages access authorization policy

3.13
policy information point
service that acts as the source of attributes for a PDP to make authorization decisions

3.14
resource
object
physical, network, or any information asset that can be accessed for use by a subject.

3.15
subject
entity involved in access control (3.1) as holder of a privilege.

3.16
security token service
service that builds, signs, exchanges and issues access tokens based on decision made by PDP

NOTE This service may be split into separate components.

3.17
Subject centric implementation
Implementation pattern of AMS as services where subject plays a crucial role.