FINAL
DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 24643

ISO/IEC JTC **1**

Secretariat: ANSI

Voting begins on:
2020-08-18

Voting terminates on:
2020-10-14

Architecture for a distributed real-time access system

This document is circulated as received from the committee secretariat.

FAST TRACK PROCEDURE

Reference number
ISO/IEC FDIS 24643:2020(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Overview 1

5 Functional architecture of an access system 3
5.1 Physical function group 3
5.1.1 Components 3
5.1.2 Access object 4
5.1.3 Access point 4
5.2 Network layer 5
5.2.1 Components 5
5.2.2 Edge 5
5.2.3 Telecommunication network 5
5.3 Service function group 5
5.3.1 Components 5
5.3.2 Processing functions 6
5.3.3 Transaction data 6
5.4 Platform function group 6
5.4.1 Components 6
5.4.2 Policy function 7
5.4.3 Authentication and access object data 7
5.4.4 System data 7
5.4.5 Inter applications 7

6 Interfaces 8
6.1 Physical function group and network function group 8
6.2 Network function group and service function group 8
6.3 Service function group and application function group 8
6.4 Inter applications 8

Annex A (informative) **Example of the data format** 9
A.1 Transaction data 9
A.2 Authentication and access object data 9
A.3 System data 10

Annex B (informative) **Example of complicated authentication** 11
B.1 Enter an important facility 11
B.2 Electronic voting system for election 11
B.3 Authentication process 12

Bibliography 13

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Ecma International (as ECMA-417) and drafted in accordance with its editorial rules. It was assigned to Joint Technical Committee ISO/IEC JTC 1, *Information technology*, and adopted under the "fast-track procedure".

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Technology for real-time access control is widely used in many situations such as facility entrance systems in a building, payments at a hotel, ATM operations or e-voting in an election, etc. These services benefit from real-time access control systems connected via networks and using database information.

Sophisticated cloud, virtualization, database, networking technology and services and the evolution of authentication technology such as biometrics, NFC, QR codes used in distributed and modular access control systems enable previously underserved users and operators to innovate around new use cases.

For realizing such real-time access system, an Ecma standard ECMA-412 (also published as International Standard ISO/IEC 20933) "Framework for distributed real-time access systems" was first introduced in 2016 with a 2nd edition following in 2018. That standard specifies the reference model and common control functions. It gives direction for ongoing innovation and development of technology and the system integration of distributed real-time access control systems.

This Standard specifies the architecture for a distributed real-time access system taking into account the many technologies and the framework of ECMA-412. The architecture specifies the function group concept of the system, the functionalities of each function group and the interfaces. Protocols between function group and functions are out of the scope of this Standard.

This 2nd edition introduces some clarifications and editorial improvements to the text.

This Ecma Standard was developed by Technical Committee 51 and was adopted by the General Assembly of June 2019.

Architecture for a distributed real-time access system

1 Scope

This Standard specifies the architecture for a distributed real-time access system. The architecture specifies the function group concept of the system, functionalities of each function group, and interfaces. Communication between function group and functions are not in the scope of this Standard.

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.

ECMA-412, *Framework for distributed real-time Access systems*

ISO/IEC 20933, *Information technology — Distributed application platforms and services (DAPS) — Framework for distributed real-time access systems*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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 https://www.iso.org/obp

3.1
access ID
identifier of an access request

3.2
access object
physical entity which access the access system

3.3
access object ID
identifier of an access object

3.4
access point
object ID receiver from access object for starting access system activities and an access system activity final result receiver for completion of the activities

3.5
access point ID
identifier of an access point

3.6
edge
boundary between pertinent digital and physical entities, delineated by networked access points

Note: see ISO/IEC TR 23188

3.7
edge node ID
identifier of an edge

3.8
transaction
suite of functions and message exchanges to generate a final result and sent to a receiver (Source: ISO/IEC 20933)

4 Overview

A distributed real-time access system, as described in ECMA-412 and ISO/IEC 20933, (hereafter; access system) is a system which decides in a timely manner to permit or deny access from an access object and proceed with an access system service after access is granted. The access points of the system are spatially distributed. An access system will be activated by the access of an access object at the access point. After its validity confirmation, authentication, some services of the access system will proceed serially and/or parallelly. When the processing of all the services is completed, the service result is sent back to the access point. During such transaction, the series of action should be authenticated through an authentication process, logically and physically as illustrated in Figure 1.

Figure 1 shows an access system activity flow for an access system which is activated by the access object access at the access point to the end of the series of actions of the system. In Figure 1, the blue arrow shows the message(s) flow from the access object to the access point, access point to the processor and any processor to any other processors. Those object ID messages from the access object to the access point are used to process results messages to Process 1 and so on. At any process functions, based on the received messages, each process function performs various processing. The message results of each process, are accepted or denied, (process complete or incomplete), and the result related ID(s) are sent to the next processing function.

All of the processing result messages from Process 1 to process N-1 are sent to Process N function, final judgement process, which decides of the final result, accept or deny. Then, the final result is sent to the access point as a receiver of the result and completes a transaction and access system activity. If the result of any processing function is ”deny” at any steps of an access system activity, such messages are sent to the final judgement process. Then, the final result is judged as “deny” by the final judge process function. The “deny” message is sent to the receiver and completes the transaction and access system activity.

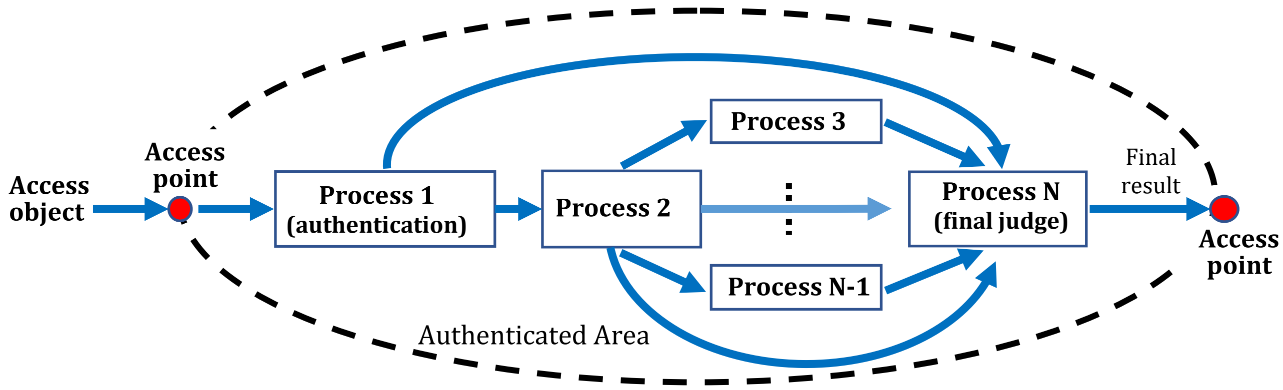

Figure 1 — Access System Behaviour

The rules of message management and procedures of the system activities are provided by policy in the policy function (Figure 3) of the platform function group. Those rules vary and depend on the services and applications of each access system. Furthermore, the direction management rules of the messages from each process are also provided by policy function and based on the rules., The message from the access point sent to an appropriate process function is managed by an edge node. Access point result messages will send through edge node to authentication process in the service function group. (Figure 3)

Activities of each process functions are out of the scope of this standard.

Figure 2 shows an example, a hotel-check in process. There are many rooms in a hotel and each room entrance access point is locked. An access object is a human in this case, who has a key card with an object ID. When the person inserts or touches the key card at the entrance door, the access point receives an object ID from key card then an access system, which includes an authentication process starts. If the key card was authenticated at the hotel front desk, the authentication result, final result, requesting access is accepted and an open the door message, final result, goes to the access point, then, the door will open. If the key card is not authenticated, access request denied through the authentication process and the door will not open. The access system activity is then completed.

Note: in this example, configuration of key card, ID messages in the key card, key card reader, activities of door open, or close mechanism, etc. are out of the scope of this standard.

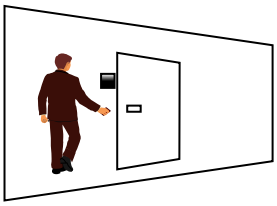

Figure 2 — An example of hotel room check-in

This is a very simple example, but there are many kinds of such access systems. Some systems have very large number of access points, some systems have widely distributed access points, some systems require complicated authentication. Annex B shows some examples of complicated authentication. In order to construct or implement an access system, the following are important issues and they could be done in many different ways. Those are out of scope of this Standard.

— in the case that the system has widely distributed access points, the data management processing is important when many access objects access large number of access points at the same time. The total processing time should be shortened to a few second or less;

— flexibility and expandability are also important, such as easy updates of the number of controlled access points, number of users and its data, system configuration and its software, including rules, etc.

This Standard clarifies the requirements of these access systems, and shows a functional architecture and interfaces. Figure 3 shows the functional architecture of the access system.

Note: multi-layer functions, such as security, privacy and governance, are out of the scope of this standard.