INTERNATIONAL STANDARD

ISO/IEC 20933

First edition
2016-05-15

Information technology — Distributed Application Platforms and Services (DAPS) — Access Systems

Technologies de l'information — Services et plate-formes d'application distribuées — Systèmes d'accès

Reference number
ISO/IEC 20933:2016(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
Web www.iso.org

Published in Switzerland

Contents

Page

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.

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. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

ISO/IEC 20933 was prepared by Ecma International (as ECMA-412) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Introduction

Technology for real-time access control is widely used for many situations such as entrance gate of facilities and service access control systems. Membership and settlement services also benefit from real-time access control systems connected via networks and using database information.

Sophisticated cloud, virtualisation, 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.

Taking into account the many technologies, this International Standard specifies the reference model and common control functions. It gives direction for ongoing innovation and development of technology and system integration of distributed real-time access control system.

Information technology — Distributed Application Platforms and Services (DAPS) — Access Systems

1 Scope

This International Standard specifies:

1) an ID triggered modular access system, the functions of the modules and the messages they exchange, and the sequence of messages, i.e. transitions of the transaction;

2) the system responsibility from receiving an access request until sending the result. i.e. a complete transaction;

3) the responsibilities of the modules, including time stamping and responding to the requests they received; and

4) the sequence and semantics of the messages and their elements.

2 Conformance

Conformant Access Systems progress transactions by evaluating the applicable rules. Conformant modules implement the requests on their interfaces, the corresponding responses and time stamping as specified herein.

3 Normative references

None.

4 Terms, definitions and acronyms

For the purposes of this document, the following terms, definitions and acronyms apply.

4.1
ID
Identifier

4.2
RED
Rule Evaluation and Dispatching

4.3
transaction
request for access

5 Model

Figure 1 illustrates the Access System structure.

The Access System has 5 modules "Access-point, Policy, Processing, RED and Storage" and 4 interfaces "Access-interface, Policy-interface, Processing-interface and Storage-interface".

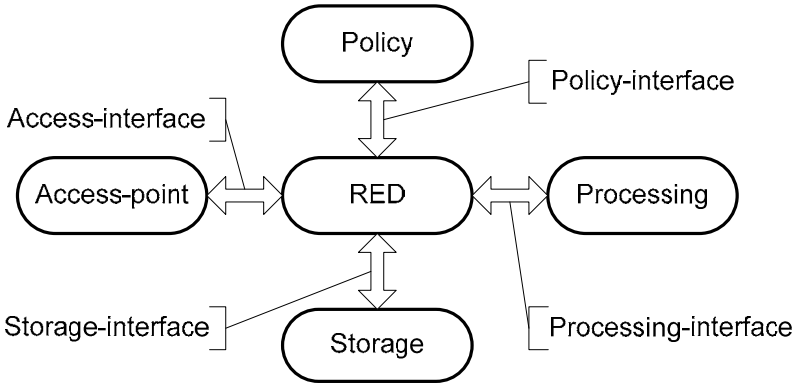

Figure 1 — Access System

The Access System progresses a transaction by exchanging messages between modules and decides the final result (grant or deny). A transaction starts when an Access-point module obtains Access_request and completes when the RED module sends Final_Result_Notification. Each module shall have a time stamping function. The message exchanging and the time stamping function are managed by the RED module according to rules which are set by the Policy module.

6 Transaction

Transaction ID identifies a transaction. Transaction ID shall consist of Access ID, Access-point ID and time at which the Access_request is obtained. Access ID is included in Access_request.

Figure 2 specifies the state machine of a transaction.

A transaction is generated at the time of Access_request acceptance by an Access-point module. After that the transaction changes to on-going state by sending a Transaction_start_request including Transaction ID from the Access-point module to the RED module.

At the on-going state, the RED module evaluates rules until final result is obtained. According to the result of the evaluation, the RED module sends a request message to Processing or Storage module and receives a response message.

When the RED module obtains the final result, it sends Final_Result_Notification and the transaction is completed.

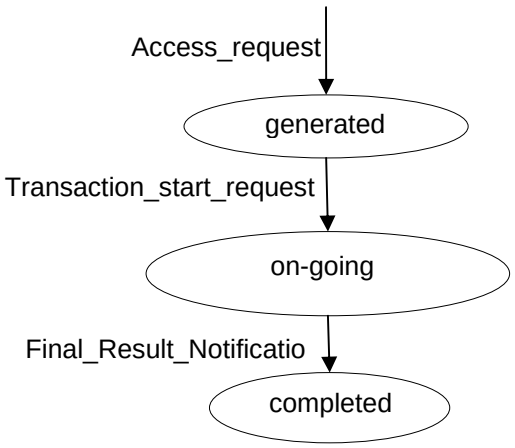

Figure 2 — Transaction State Machine

7 Time stamping function

The purpose of Time stamping function is to measure the duration of transaction and request processing.

The Access-point modules shall set the Access_ID_obtained_time in the Transaction_start_request message. For the other modules, time stamping shall be activated and deactivated through time stamping rules. Upon evaluating of the time stamping rules, the RED module shall set the TimeStampingFlag value in the requests to TRUE or FALSE according to the evaluation. Depending on the TimeStampingFlag value in the requests, modules shall either time stamp the ReceivedTime and SendingTime or exclude those elements in the corresponding response.

The RED module shall send the time stamping measurements by responding to the Time_stamp_Notification.

The RED module is able to measure following time.

1) transaction processing time

2) request processing time.

When the Time stamping function of each module is activated, the RED module shall measure the following time.

3) module processing time.

The RED module shall measure the transaction processing time by calculating the difference between the time that the RED module received Transaction_start_request and the time that Final_Result_Notification is sent.

The RED module shall measure the request processing time by recording the sending time of the request and the received time of the response, and calculating the difference between them.

Processing_response, Store_response and Retrieve_response have the information about the received time of the corresponding request and the sending time of the response itself as long as the Time stamping function is activated. By using them, the RED module is able to measure the module processing time. For example, the module processing time of the Processing module for one request from the RED module is measured by the difference between RecievedTime and SendingTime in the corresponding Processing_response.

Annex C illustrates the usage of time stamping.

8 Module

8.1 Common requirements

Modules shall have a time stamping function.

8.2 Policy module

The Policy module shall have the source of rules, and shall set the rules to the RED module. Each rule shall be identified by its Rule ID. The rules shall define the progress of transactions and the edition of this International Standard that the Access System modules conform with. And the rules shall identify the receiver(s) of the Final_Result_Notification and the receiver(s) of the Time_stamp_Notification.

8.3 Access-point module

When an Access-point module obtains an Access_request, It shall generate a Transaction_start_request and send it to the RED module.

The Access-point module shall have its own identifier as Access-point ID.

8.4 RED module

The RED module shall accept and hold rules that are set by the Policy module.

Rules are composed of procedure rules and branch rules, Figure 3 illustrates a procedure rule and Figure 4 illustrates a branch rule. A procedure rule determines the next execution. A branch rule selects the next rule depending on the branch condition. At least one rule is linked to Access ID.

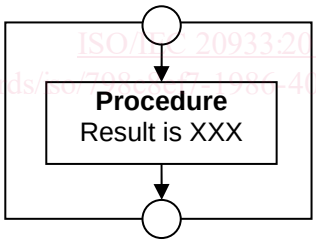

Figure 3 — procedure rule

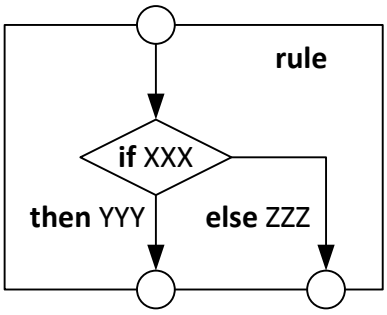

Figure 4 — branch rule

During a transaction, the RED module is driven by messages. When the RED module receives messages, It shall evaluate the rules. The RED module shall dispatch the request and response from one module to