ecma INTERNATIONAL

Standard ECMA-417

1st Edition / December 2018

Architecture for a distributed real-time access system

Standard

Rue du Rhône 114 CH-1204 Geneva T: +41 22 849 6000 F: +41 22 849 6001

is the registered trademark of Ecma International

Contents

Page

Introduction

The 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 technologies and services and the evolution of authentication technologies 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 [1] (also an International standard ISO/IEC 20933 [2]) “Framework for distributed real-time access systems” was introduced in 2016 and revised in 2018. This 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 reference architecture for a distributed real-time access system taking into account the many technologies and the framework of the ECMA-412 standard [1]. The reference architecture specifies the layer concept of the system, the functionalities of each layer and the interfaces. Protocols between layers and functions are outside the scope of this Standard.

This Ecma Standard was developed by Technical Committee 51 and was adopted by the General Assembly of December 2018.

Architecture for a distributed real-time access system

1 Scope

This Standard specifies the reference architecture for a distributed real-time access system. The architecture specifies layer concept of the system, functionalities of each layer, and interfaces. Protocols between layers and functions are excluded of this Standard.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

3.1
access object
physical entity to access to the access system

3.2
access ID
identifier of an access request

3.3
access point ID
identifier of an access point

3.4
edge ID
identifier of an edge

3.5
personal ID
identifier of an access object

4 Overview

A distributed real-time access system, as described in ECMA-412 [1] and ISO/IEC 20933 [2], (here after; access system) is a system which decides in a timely manner to permit or deny access from an access object and proceeds with an access system service after access is granted. Access points of the system are spatially distributed. An access system will be activated by the access object access at the access point and after its validity confirmation, authentication, some services of the access system will proceed serially and or in parallel. After processing all the services, the service result is sent back to the access point after which the transaction will be completed. During a transaction, the series of actions should be secured through an authentication process, logically and or physically. Figure 1 illustrates this behaviour.

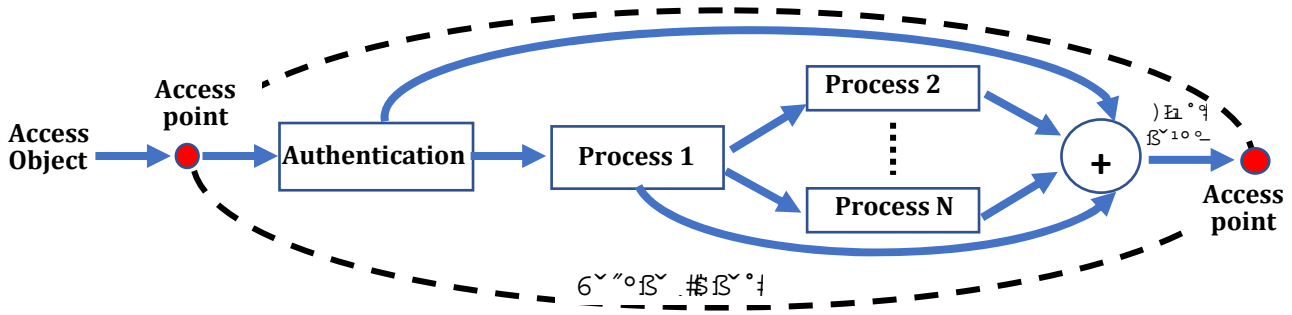

Figure 1 — Access system behaviour

Figure 2 shows an example. There are many rooms in a hotel and each entrance of a room is locked. An access object is a human in this case, who has a key card. When the person inserts or touches the key card at the entrance door, in the case the key card was authenticated at the hotel front desk, the door will be open, and if the key card was not authenticated, the door will not be open.

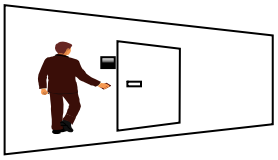

Figure 2 — An example of hotel room check in

This is a very simple example, but there are many kinds of such access systems. Some systems have very large numbers of access points, some systems have widely distributed access points, some systems require complicated authentication. Annex B shows some examples of a complicated authentication. In the access system, the data management process when many access objects access large numbers of access point at the same time, shortening the total processing time, within a few second or less, is essential. For a system, which has widely distributed access points, system flexibility and expandability, such as easy updates of the numbers of controlled access points, number of users, its data, system configuration, software and rules are the important issues and they could be done in many different ways. Those are, however, out the scope of this Standard.

This Standard clarifies the requirements of these access systems, and then shows a functional reference architecture and interfaces. Figure 1 shows the functional reference architecture of the access system.

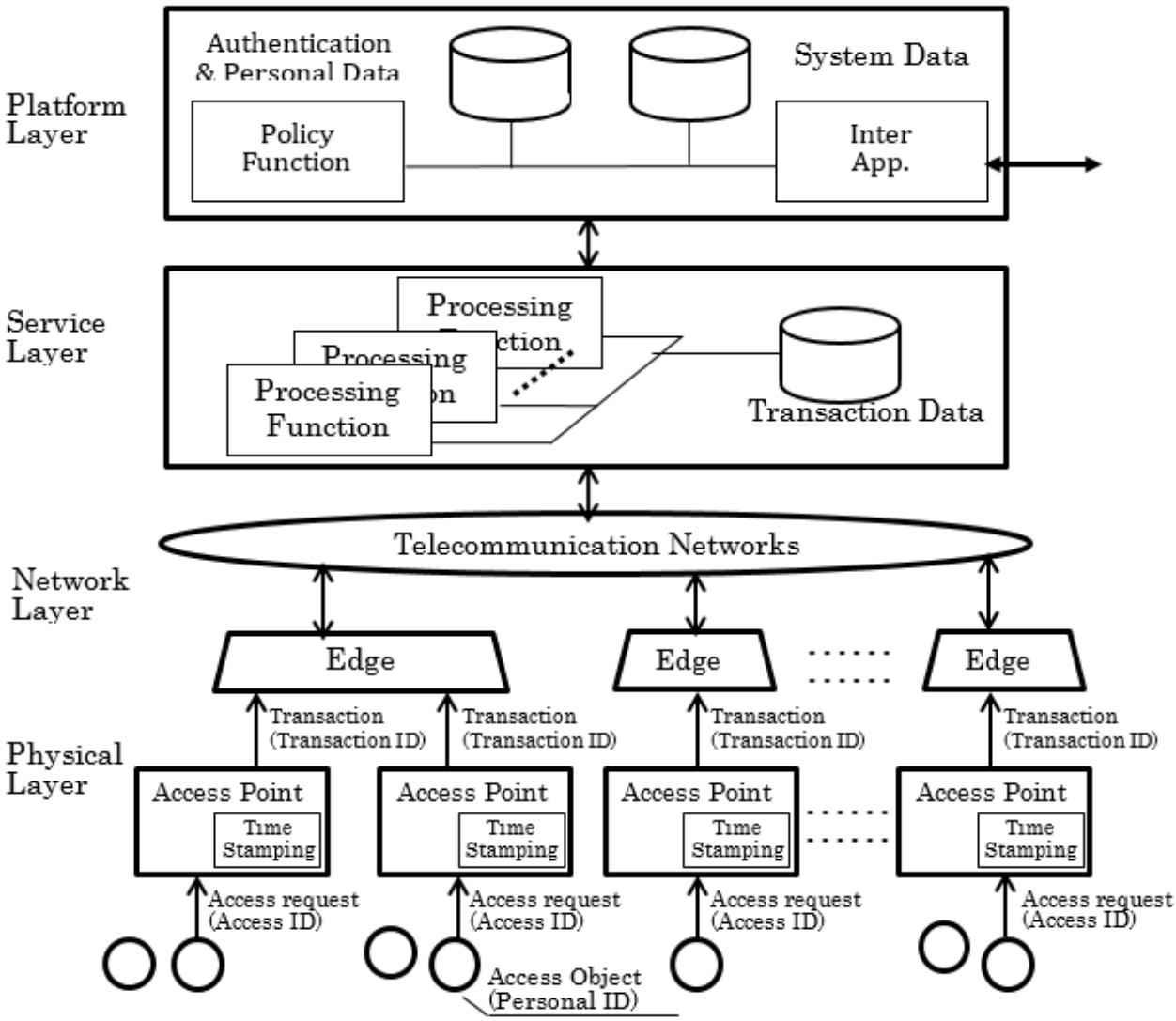

Figure 3 — Functional reference architecture of the distributed real-time access system

5 Requirements

5.1 Physical layer

There are access objects and access points in the physical layer of the access system.

The access object is required to have a unique identifier. This ID is given to an access object User and or customer from the service provider when contracted. The life of this ID depends on the contract and it is out of scope of this Standard.

The access point is required to have an identifier such as an access point number. The access point shall receive the access request of the access object independently from accepting the request or denying the request.

The access point should generate an access ID to link the personal ID of the access object with the access. The access point shall generate a transaction with a transaction ID to start the process in the access system.

The transaction shall be a data set of a transaction ID, access point ID, access ID, and personal ID. The transaction should have a time stamp to indicate the starting time of the process. The access point should process the access requests one by one.

The access point should sometimes have a receiver function to handle the result of the transaction originated by one access request from the access object. The result maybe, for example, the opening of a door/gate, displaying of a payment settlement, completion of a voting procedure, etc. at an access point, physically.

5.2 Network layer

There are telecommunication networks and edge functions in the network layer.

The telecommunication networks shall transfer transactions that each access point generates to the service layer which is described in 5.3. Network protocols are out of the scope, but the protocol should be simple and light because the processing time for a transaction should be several seconds or less considering a so-called real-time system.

Network speed is also very important for specific applications.

The edge function should help to process a large number of transactions. Traffic concentration and memory cashing should be required at the edge functions to decrease burden on the networks. The required functions are described in 6.2.1. Each edge function should have the edge ID to identify which access point is connected to the edge.

Edge should have the functions of checking if the access point is an authorized one, physically and logically and monitors the access point capability.

5.3 Service layer

The service layer includes common functionalities of the access system. The processing and storage functions shall process transactions to decide the access acceptance/denial and to proceed with the services of the access system of the linked access request. To realize real-time processing these functions should be implemented using parallel processing technologies.

However, in most of the case, the access authentication process is executed first and then, other processes for services/applications of an access system will be processed.

The transaction related data including not only authentication results and some processing results, but also access point IDs, access IDs, personal IDs, and time stamps shall be stored in this layer as transaction data sorted by transaction IDs.

5.4 Platform layer

There are policy functions which indicate how to process transactions according to each application. There is a system data policy which stores the system structure including access point locations, operation status, and related edge IDs sorted by access point IDs. Finally, an authentication and personal data policy function which stores personal data according to applications and authentication status that decides the acceptance/denial of the access request. The authentication and personal data should include charging data to pay access fees and subscribing information of the application including expiration date and time of the application. The authentication and personal data are sorted by personal IDs. In the platform layer, there should be an inter application interface to provide access objects who subscribe to a plural number of different applications to process with access transparency.

6 Functional reference architecture of the access system

6.1 Physical layer

6.1.1 Access object

The access object is an entity that requires to access the access system. The entity may be a human or a mechanical object such as a card. The access object shall have its personal ID. The personal ID should be stored in an electronic card, an RFID, a smart phone, or another such object. Biometrics data such as a face, fingerprints, iris, veins, etc. should also be used as IDs.

The acquisition or extraction of necessary biometrics data (raw and/or characterized parameters) and the authentication of using such biometrics data depend on the access system configuration and its services are out of scope of this Standard.

6.1.2 Access point

The access point is an entrance or an exit of the access system and;

- should have a function of gateway to control the access;
- shall have a function to receive the access request from the access object;
- shall have a function to generate a transaction with a transaction ID;
- shall have a function to send the transaction to the service layer to set the transaction ID into the transaction data storage;
- shall have a function to receive a result of the authentication which is confirmed using the information in the authentication & personal data storage in the platform layer.

The access request receiving function, personal ID reader, should be implemented as an electronic card reader, a sensor for a smart device, a camera for biometric data, etc.

6.2 Network layer

6.2.1 Edge

The edge function:

- shall have an edge ID;
- shall include a function of traffic concentration/distribution;
- shall include a function of data cashing to keep recent uses of both the transaction data and the authentication data.

6.2.2 Telecommunication network

The network shall have a function to dispatch transactions between the access point and the processing & storage, or the edge and the processing & storage. The network performance including latency, the error rate, etc. should be dependent on the specification of adopted application.

6.3 Service layer

6.3.1 Processing functions

The processing functions are equipped in parallel manners in the processing & storage. The processing function:

- shall include a function to manage transactions using the transaction data storage;
- shall include a function to process transactions according to the rule which defines the procedures of how to process transactions stored in the policy function of the platform layer;
- shall include a function to refer to the authentication & personal data, and the system data to decide acceptance or denial of the access request;
- shall include a function to send the result of the authentication and the result of a transaction related processing through networks (and an edge).

6.3.2 Transaction data

The transaction data are stored data and shall have information related to a transaction ID. An example of the transaction data format is shown in A.1.

6.4 Platform layer

6.4.1 Policy function

The policy function shall have a set of the sequence and procedure to process the application as a rule. The rule should be referred from the processing functions or sent to the processing functions in order to process transactions appropriately. The rule should be a kind of software program or macro command. The rule should be provided according to the adopted application.

6.4.2 Authentication & personal data

The authentication and personal data are stored data and shall have information related to a personal ID. An example of the authentication & personal data format is shown in A.2.

The authentication and personal data acquisition and registration to the storage in the platform layer set by service provider vary and it is out of the scope of this Standard.

6.4.3 System data

The system data are stored data and shall have information related to an access point ID. An example of the system data format is shown in A.3.

6.4.4 Inter applications

The inter application shall have a function to exchange the authentication and personal data among other applications. This function is for an application which uses multi-step authentication. The applications should be identified by a service identifier.

7 Interfaces

7.1 Physical layer and network layer

This interface shall specify a transaction format including the personal ID, the access ID, the access point ID, transaction ID, the type of the request, the type of the response, and the time stamp.

7.2 Network layer and service layer

This interface shall specify a transaction format including the personal ID, the access ID, the access point ID, transaction ID, the type of the request, the type of the response, and the time stamp. The edge ID should be added in the format.

7.3 Service layer and application layer

This interface shall specify a transaction format including the personal ID, the access ID, transaction ID, the type of the request, the type of the response, and the time stamp.

7.4 Inter applications

This interface shall specify a transaction format including the personal ID, the access ID, the access point ID, transaction ID, the service identifier, the type of the request, the type of the response, and the time stamp.

Annex A
(informative)

Example format of the data

A.1 Transaction data

Table A.1 — Sample format of the transaction data

Transaction ID	Access ID	Personal ID	Request	Response	Time Stamp
9001	0101	1234	Ack	Yes	20170620081535099
9002	0102	5678	Ack	No	20170620092858216
90ee	N	Xxxx	----		
90ff	M	yyyy	----		

A.2 Authentication & personal data

Table A.2 — Sample format of the Authentication & Personal Data

Personal ID	Services	Authenti-cation	Transaction ID	Expire Date
0001	A	Yes	0101	2018-05-31
0002	A	No	0102	2020-12-31
xxxx	N	No	----	
yyyy	M	Yes	----	

A.3 System data

Table A.3 — Sample format of the System data

Access point ID	Edge ID	Location	Operation	Notes
000001	001	A01F03	Active	
000002	002	B02G05	N/A	
pppppp	Nnn	C04L09	----	
qqqqqq	mmm	D03K08	----	

Annex B
(informative)

Example of complicated authentication

B.1 Enter an important facility

In the case of entering an important facility, such as a nuclear power plant, airport, etc., at least two authentication processes are needed. Those are hazardous material check to assess if a person carries hazardous materials (such as explosives, gas, knife, weapon, drugs, alcohol, etc.) and a human authorization to verify that the person is authorized to enter the facility.

In this case, an access object is a human who has an ID card or biometric data.

When a person comes to the gate, access point, the hazardous material check is processed physically. If no hazardous material is found or detected, this access request is permitted.

In parallel or serial of this authentication process above, the human authentication process is executed.

At the entrance gate, a person will insert or touch the ID card or show their face, finger print, iris, etc. to the biometric data reader or camera. If the ID card or the biometric data is authorised by the security office of the facility, the person is allowed to enter the facility.

Together with two authentication results accepted, the gate at the access point opens.

If one of two or two authentication results deny the access, the gate does not open.

In some cases, there are two separate gates for evaluating each item independently, and in some case, there is one gate for evaluating both items at once.

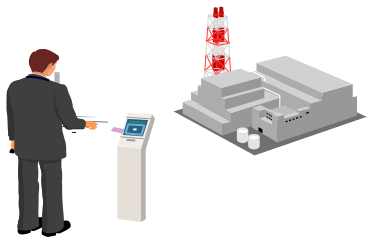

Figure B.1 — Enter the Important facility

B.2 Electronic voting system for elections

In the case of an electronic voting system, the voting machine is the access point for voting and has the functions of authenticating the voting person and recording the vote for an election. These functions are sequentially executed. The voter authentication process is the same as above in example B1. The only difference is that the authentication data of each voter is assigned by a government in advance of the election.

When a voter comes to the voting machine and touches or inserts the ID card in the machine, the voting person authentication process is executed. If the voter is authorized and accepted for voting, the voter can

vote a candidate from the list. After the voting, the voter can confirm the votes on the display of the voting machine.

Figure B.2 — Electronic voting system

B.3 Authentication process

When an access object (e.g. ID card) with authorized data access to an access point requests an access system to operate certain application services, an authentication process takes place. The access point reads the personal ID of the access object and sends such data to a service layer through a communication network. At the service layer, the authentication process will be executed using the data from the access point and the authentication data from the platform layer. The final result of an authentication is to accept or deny access to the service.

Furthermore, in some cases, to create a more effective access system (e.g. a shorter service transaction time), the authentication process may be performed at the physical layer in the access point. The implementation of such system depends on the access system services and/or applications and is out of the scope of this Standard.

Bibliography

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

[2] ISO/IEC 20933*, Information technology — Distributed Application Platforms and Services (DAPS) — Framework for distributed real-time Access systems*