ecma INTERNATIONAL

Standard ECMA-417

3rd Edition / August 2021

Architecture for a distributed real-time access system

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

Contents

Page

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 layer concept of the system, the functionalities of each layer and the interfaces. Protocols between layers and functions are out of the scope of this Standard.

The 2nd edition introduced some clarifications and editorial improvements to the text.

This 3rd edition is fully aligned with ISO/IEC 24643:2020 and introduces Central Bank Digital Currency (CBDC) and vaccine passports as additional examples of complicated authentication in Annex B.

This Ecma Standard was developed by Technical Committee 51 and was adopted by the General Assembly in August 2021.

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 Standard, the following terms and definitions apply.

3.1
access ID
identifier of an access request

3.2
access object
physical entity which access the access system

3.3
access point ID
identifier of an access point

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.

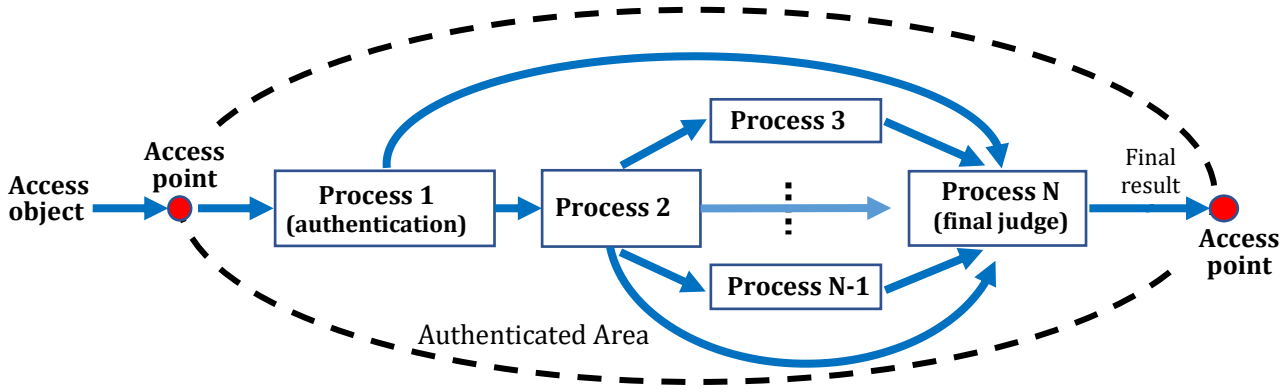

Figure 1 — Access System Behaviour

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.

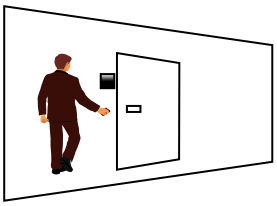

Figure 2 — An example of hotel room check-in

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.

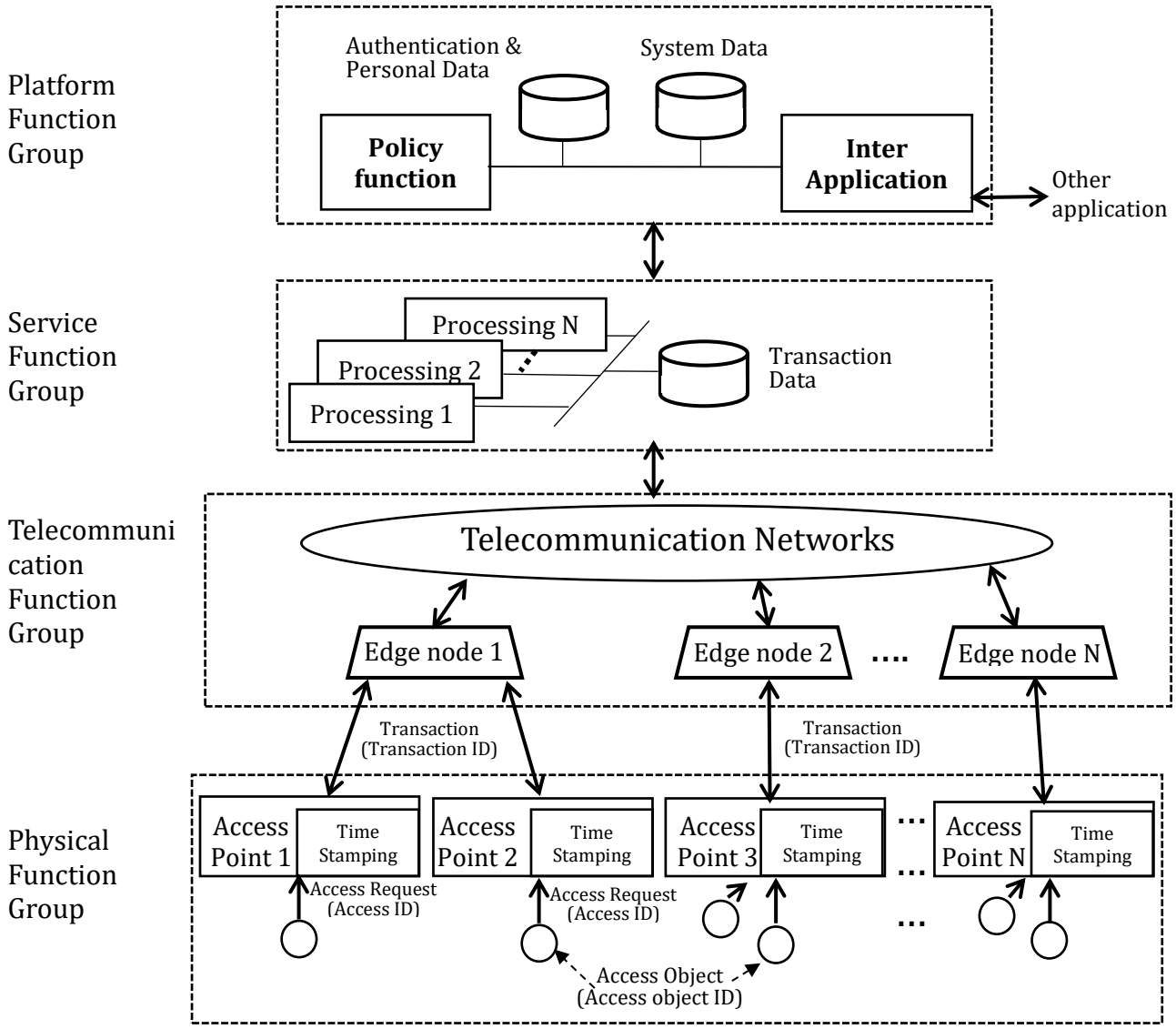

Figure 3 — Functional architecture of access system

5 Functional architecture of an access system

5.1 Physical function group

5.1.1 Components

There are access objects and access points in the physical function group of an access system.

5.1.2 Access object

5.1.2.1 Functions

Access object is an entity to require access to the access system. The entity may be a human or a mechanical object such as a card. Each access object has its access object ID. The access object ID is given to a user

and/or customer of the access object from the service provider when contracted. The life of access object ID depends on the contract of the access system service and is out of the scope of this Standard.

5.1.2.2 Requirements and recommendations

The access object ID shall be unique in this access system.

The access object ID should be stored in an electronic card, an RFID, a smart phone, or another such object.

Biometrics data such as face, fingerprint, iris, veins recognition, etc. should also be used as IDs. The way of necessary biometrics data (raw and/or characterised parameters) acquisition or extraction and the way of authentication using such biometrics data depend on the access system configuration and its service. Such authentications are out of scope of this Standard.

5.1.3 Access point

5.1.3.1 Functions

An access point represents the entrance and/or the exit of the access system and:

— has an access point ID;

— has a function of physical gateway to control an access;

— receives an access request from an access object;

— generates an access ID to link the access object ID of the access object with the access;

— generates a transaction ID;

— generates a transaction to start the process in the access system. A transaction is a data set of a transaction ID, access point ID, access ID, access object ID and a time stamp to indicate the process starting time;

— sends the transaction to the service function group via the network function group;

— receives a result of the authentication which is confirmed in the platform function group;

— sometimes has a function of the receiver of the result of the transaction originated by an access object. The result may be, for example, opening a door/gate, displaying payment settlement, the completion of the voting, etc. at the access point, physically.

5.1.3.2 Requirements and recommendations

The access point ID shall be unique in this access system.

The access point shall receive the access request of the access object independently from the acceptance or denial of the request.

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

The access ID shall be unique in this access system.

The transaction ID shall be unique in this access system.

The access point should process the access request one by one.

5.2 Telecommunication function group

5.2.1 Components

There are telecommunication networks and edges in the telecommunication function group. Edges may be optional in some applications and access systems.

5.2.2 Edge

5.2.2.1 Functions

The edge helps to process a large number of the transactions to decrease burdens of the networks and;

— has an edge node ID to identify which access point is connected to the edge;

— includes a function of traffic concentration/distribution;

— includes a function of data caching to keep recent uses of both the transaction data and the authentication data;

— may have the functions of checking the access point if it is authorized physically and logically, and monitoring the access point capability.

5.2.2.2 Requirements and recommendations

The edge node ID shall be unique in this access system.

5.2.3 Telecommunication network

5.2.3.1 Functions

The network has a function to dispatch transactions between the access point and the processing and storage in the Service function group, or the edge node and the processing and storage.

5.2.3.2 Requirements and recommendations

The network performance including latency, throughput, error rate, etc. should be decided taking into account the adopted application specification.

The network protocols are out of the scope of this Standard, but the protocol should be simple and light enough because the processing time for a transaction is supposed to be several seconds or less considering a so-called real-time system.

5.3 Service function group

5.3.1 Components

The service function group includes common functionalities of access systems, namely, the processing functions and transaction data, to decide the acceptance or denial of the access and to proceed other services of the access system of the linked access request.

5.3.2 Processing functions

5.3.2.1 Functions

The processing function:

— manages transactions using the transaction data;

— processes transactions according to the rule stored in the policy function in the platform-function group;

— refers to the authentication, access object data and the system data, and decides acceptance or denial of the access request;

— sends the result of the authentication and the result of transaction related processing through networks (and an edge).

5.3.2.2 Requirements and recommendations

To realize real-time processing, processing functions should be implemented using parallel processing technologies.

However, in most cases, an access authentication process should be executed first before other processes for services or applications are processed.

5.3.3 Transaction data

5.3.3.1 Functions

The transaction data are stored data which have information related to a transaction ID. The transaction itself and its related data including authentication results and some processing results are stored as transaction data. An example of the transaction data format is shown in A.1.

5.3.3.2 Requirements and recommendations

The transaction data shall be sorted by transaction ID.

5.4 Platform function group

5.4.1 Components

In the platform function group, there are following components:

— policy functions which indicate how to process transactions according to each application;

— system data which stores system structure including access point locations, operation status, and related edge node IDs sorted by access point IDs;

— authentication and ł access object data which are used to decide acceptance/denial of the access request; and

— optionally an inter application interface to provide access objects which subscribe a plural of deferent applications to process with access transparency.

5.4.2 Policy function

5.4.2.1 Functions

The policy functions have a set of the sequence and procedure to process the application as a rule. The rule is referred by the processing functions or sent to the processing functions to process transactions appropriately. The rule is provided according to the adopted application.

5.4.2.2 Requirements and recommendations

The rule should be a kind of software programs or macro commands.

5.4.3 Authentication and access object data

5.4.3.1 Functions

The authentication and personal data are stored data related to an access object ID. The authentication and access object data depend on the applications and includes, for example, charging data to pay access fees and subscribe information of the application including expire date and time of the application. An example format of the authentication and access object data is shown in A.2.

The way of authentication and access object data acquisition and registration to the storage in the platform function group set by service provider varies and it is out of scope of this Standard.

5.4.3.2 Requirements and recommendations

The authentication and access object data shall be sorted by access object IDs.

5.4.4 System data

5.4.4.1 Functions

The system data are stored data related to an access point ID. An example of the System Data format is shown in A.3.

5.4.4.2 Requirements and recommendations

There are no requirements and recommendations for system data.

5.4.5 Inter applications

5.4.5.1 Functions

The inter applications exchange the authentication and access object data among other applications. This function is for the case of an application which uses multi-step authentication.

5.4.5.2 Requirements and recommendations

The applications should be identified by a service identifier.

6 Interfaces

6.1 Physical function group and network function group

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

6.2 Network function group and service function group

This interface shall specify a transaction format including the access object 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 node ID shall be added in the format, if any.

6.3 Service function group and platform function group

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

6.4 Inter applications

This interface shall specify a transaction format including the access object 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 of the data format

A.1 Transaction data

Table A.1 — Sample format of the transaction data

Transaction ID	Access ID	Access object ID	Request	Response	Time Stamp
9001	1010	1234	Ack	Yes	20170620081535099
9002	102	5678	Ack	No	20170620092858216
90ee	N	Xxxx	----		
90ff	M	Yyyy	----		

A.2 Authentication and access object data

Table A.2 — Sample format of the authentication and access object data

Access object ID	Services	Authentication	Transaction ID	Expire Date
0001	A	Yes	0101	2018-05-31
0002	A	No	0102	2022-12-31
xxxx	N	No	----	
yyyy	M	Yes	----	

A.3 System data

Table A.3 — Sample format of the system data

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

Annex B
(informative)

Examples of complicated authentication

B.1 Enter an important facility

In the case of entering an important facility, nuclear power plant, airport, etc., at least two authentication processes are needed. Those are hazardous material check if the person carries hazardous materials such as explosives, gas, knifes, weapons, drugs, alcohol etc. and human authorization if he or she is an authorized person to be able 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 performed physically. If no hazardous material is found, or detected, this access request is permitted.

In parallel or serial of this authentication process, 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, 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 is or are access denied, the gate does not open.

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

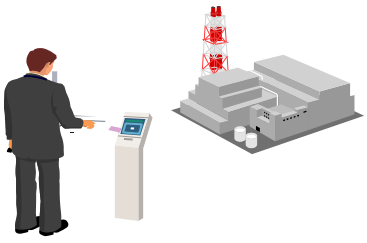

Figure B.1 — Enter the Important facility

B.2 Electronic voting system for election

In the case of an electronic voting system, the voting machine is the access point for voting and has the functions of authenticating the person that votes and voting for the election. These functions are sequentially executed. The voter authentication process is the same as above in example B.1. The only difference is the authentication data of each voter is assigned by a government entity in advance of the election.

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

from the list. After voting, the voter can confirm his or her vote on the voting machine display and complete the voting.

Figure B.2 — Electronic voting system

B.3 Authentication process

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

The examples in B.1 and B.2 assume that access objects and access points are legitimate and can be used. On the other hand, in order to make the system more secure for the execution of some services, in addition to the authentication function to check whether the access object is a legitimate user (as shown in B.1 and B.2), the service function group may also provide another authentication function to ensure the validity of the accessor and access point.

In such case, when a service start request is received from an access object via an access point, before going to the service execution process, an authentication is performed by checking the identities of the access object, the accessor itself, and the access point, and checking that each IDs which are already registered in the platform function match. As a result, if it is judged that every identity is legitimate, the service execution permission is issued and moved to the next service execution process.

The use and operation of personal information, such as identity of accessor, is governed by the privacy laws and regulations of each country and therefore details its usages are outside the scope of this Standard.

Some examples with multiple authentication functions are shown in B.4 below.

B.4 Another complicated authentication example

Examples of Central Bank Digital Currency (CBDC) or vaccine passport are systems with a large number of access points where many people can perform these services at the same time.

To prevent identity theft and fraudulent use, these systems have several authentication functions for the service requestor (accessor and access object) and the service terminal (access point) that receives the request. And only after the authentication is completed, the service process can take place.

B.4.1 Central Bank Digital Currency (CBDC)

CBDC is a system being considered by a number of countries and institutions for processing digital currency transfers among central bank, banks, companies, governmental entities and individuals where the central bank is involved directly or indirectly or in an intermediate hybrid way. It is also being considered for extensions to person-to-person transfers.

An example of a CBDC system is where an individual smart phone (access object & digital currency sender) accesses a bank terminal (access point & recipient of digital currency) to transfer digital currency.

The CBCD system verifies that the identity of the smartphone user, the smart phone and the bank terminal used are legitimate identities that are registered in the system.

After confirming all those authentications, the final confirmation of the process execution is obtained from all parties involved and the digital currency transfer is executed.

The details of technologies, operation, management, etc., of CBDC systems to ensure secure currency transfers are outside the scope of this Standard.

B.4.2 Vaccine passports

The vaccine passport, a digitalized certificate of vaccination for individuals being considered by countries and organizations, is used, for example, in a pandemic situation, to check vaccination records of individuals and allow its holder to access some services. International travel is a logical application for a vaccine passport where travellers would be checked before boarding a plane and as a part of the airport passport control process.

In the example of using an individual's smartphone as a vaccine passport, the identity of the individual (the smartphone user), the smartphone and the passport control terminal are authenticated by matching the information in the system.

After confirming all those authentications, the personal vaccination record of an individual is displayed in a secure manner on the passport control terminal.

The details of such system realization, operation, management, etc. of a vaccine passport system is outside the scope of this Standard.

Bibliography

[1] ISO/IEC TR 23188, *Information technology — Cloud computing — Edge computing landscape*