INTERNATIONAL STANDARD

ISO 37180

First edition
2021-08

Smart community infrastructures — Guidance on smart transportation with QR code identification and authentification in transportation and its related or additional services

Infrastructures urbaines intelligentes — Lignes directrices relatives au transport intelligent utilisant l'identification et l'authentification par QR code dans le domaine du transport et de ses services connexes ou supplémentaires

Reference number
ISO 37180:2021(E)

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

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 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 Technical Committee ISO/TC 268, *Sustainable cities and communities*, Subcommittee SC 1, *Smart community infrastructures*.

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

Quick Response (or QR) codes are widely used worldwide due to their extremely large capacity for data storage and data transfer instead of barcodes. In the transportation field, QR codes have been used for over 20 years. However, their application is limited since the identification and authentication procedure with QR codes in data transfer takes over one second. In cities, a ticket inspection gate should communicate with 60 customers per minute for their ticket validation at rail stations. As the number of people delayed due to ticket processing in a concourse increases, this results in more risk leading to passenger injuries. A typical example is the metro in Bangkok, Thailand. The slow processing rate of ticket inspection machines disturbs passenger flows in the station. The passengers are delayed frequently at the gate due to the processing resulting in missed trains.

In the past, the security of QR codes was very limited, and so it was highly risky to use the QR code for ticket value information retention. If the QR codes were falsely duplicated, the copies would work as a valid ticket. Transportation operators were hesitant to apply QR codes in ticketing and used the code only for specific purposes or particular situations. For example, a bus stop numbered ticket for fare adjustment in bus services and seat reservation sold within one hour of train departure.

However, the lack of security features has been overcome by improving QR code identification and authentication procedures through the use of dynamic encryption keys and their matching fields. These processes aid in achieving fluidity enhancement, controllable anonymity, non-forgery, non-repeatable data transfer and non-repudiation. QR codes are now effective tools to identify data senders and recipients. Further, QR codes can be used to authenticate information contents and authorize personal status, by completing the procedures safely and quickly. This advanced performance and security cultivate improved transportation and its related or additional service fields, such as money transfer services for payment and charging pre-paid cards. Thereby, ensuring that the services are more beneficial for customers and assist service agents with the more highly accurate and functional informational data flow. In geographic information systems where large data are traded, supported with such efforts, QR code applications already started for data provenance indication, metadata linkage, dictionary organization, data integration, qualification and exchange as well as security.

This guidance document describes QR code identification and authentication to be applied in such services.

In the development of this document, ISO Guide 82 has been taken into account in addressing sustainability issues.

Smart community infrastructures — Guidance on smart transportation with QR code identification and authentification in transportation and its related or additional services

1 Scope

This document provides guidance on transportation and its related or additional services using quick response (QR) codes for identification and authentication in data transfer, in order to make their services both convenient and advantageous for customers and service agents while protecting them from cheating and illegal action in data transfer.

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.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
QR code
<smart transportation> quick response (QR) code, such ones as designated in ISO/IEC 18004, which is to be used for identification and authentication in data transfer in or for smart transportation in a general meaning defined in ISO 37154:2017, 3.7

Note 1 to entry: Smart transportation in a general meaning is transportation that provides city issue solutions by transportation system.

Note 2 to entry: In smart transportation, data are usually transferred between customers and service agents in transportation and its related or additional services and between the agents.

Note 3 to entry: QR codes designated by ISO/IEC 18004 should be used in smart transportation. When using other QR codes not covered by ISO standards, the user would be charged on the utilization even while such QR codes still technically work for smart transportation.

3.2
QR code identification
process to identify data senders and recipients with *QR codes* (3.1) when transferring data in transportation and its related or additional services

3.3
QR code authentication
process to authenticate information contents with *QR codes* (3.1) when transferring data in transportation and its related or additional services

3.4
QR code authorization
process to authorize personal status by *QR code* (3.1) identification and authentication in transportation and its related or additional services

3.5
service agent
person working for operators, administrators and facilities owners in transportation and its related or additional services

4 Concept of smart transportation with QR code identification and authentication

4.1 Background

In transportation and its related or additional services, data should be transferred safely and quickly between customers and service agents for specific purposes such as fare or fee payment and receipts, seat, sleeping car and hotel room reservations and confirmation as well as delivery items and freight tracking. In this case, data sender and recipient identification and information content authentication should be completed instantaneously. Identification confirms who is who, while authentication recognizes what is whose. Identification and authentication work to verify persons and information, respectively. For example, it can be checked with a QR code printed on a ticket that the ticket is valid, held by a qualified person and fixed for the fare and fee payment to transportation operators. The payment can also be transacted through QR-codes, if highly secured and quickly processed.

4.2 Practical usefulness of QR codes

QR codes have good readability which is helpful in identifying persons by authenticating the content within information and retaining multiple types of information.

QR codes are applied by printing directly on paper or other materials such as plastic tickets and pasting a sticker printed therewith anywhere convenient for services (e.g. ticket vending machine bodies, transportation vehicle fee boxes, cashier counters) for identification of data senders and recipients (e.g. customers, service agents) and authentication of information contents (e.g. reservations, money transaction, enquiries). Smartphones, which are normally equipped with digital camera functions, work effectively as QG code readers and indicators. PC displays are also useful QR code indication devices, which show homepages linked to official websites for information enquiries. QR codes protect customers, if used with identification and authentication, from cheating action through phishing websites while customers are communicating therewith.

4.3 Satisfying the Sustainable Development Goals

Smart transportation works to satisfy the UN-Sustainable Development Goals (SDGs), especially goal 8 'Decent work and economic growth', goal 9 'Industry, innovation and infrastructure', goal 10 'Reduced inequalities', goal 11 'Sustainable cities and communities', goal 12 'Responsible consumption and production' and goal 15 'Life on land'.

5 QR code identification and authentication-applicable transportation and its related or additional services

5.1 General

QR code identification and authentication are normally employed as methods for highly secure data transfer. When applied in transportation and its related or additional services, they work for data senders (e.g. customers) and recipients (e.g. transportation service agents) identification and information content (e.g. reserved seats, beds and rooms) authentication. The applicable services

to customers and business work by operators, administrators and facilities owners are as already described in ISO 37154. See 5.2 to 5.6 for easy reference to the applicable services.

5.2 Services to customers in public transportation

For passenger as well as delivery items and freight services, see ISO 37154, 5.2.6.2, a) and b).

EXAMPLE QR code identification and authentication work on ticketing (e.g. seat reservation tickets) and ticket inspection (e.g. ticket verification), fare and fee payment and collection (e.g. d-payment), travel planning (e.g. service schedule download), shipping and receiving planning, delivery items and freight tracking (e.g. successful receipt), weather forecast and its information delivery, emergency communication (e.g. automatic connection), information provision and indication, and internet connection.

5.3 Services to customers in private transportation

For common and pooling vehicles, see ISO 37154, 5.2.6.3, a) and b).

EXAMPLE QR code identification and authentication work on information provision (e.g. map indication), parking lot services (e.g. parking tickets) as well as vehicle sharing and rental services (e.g. rental contracts).

5.4 Services to customers in inter-modal, carrier or line operational transportation for public and private purposes

For the same transportation mode services, inter-modal services and interface services between public and private transportation, see ISO 37154, 6.3.2, 6.3.3 and 6.3.4, respectively.

EXAMPLE QR code identification and authentication work on ticketing for travelling to other same-mode carriers and by inter-modal transport (e.g. through ticket verification between different carriers), arrangements for shipping to different-mode carriers (e.g. planning to ship to other carriers) and parking lot services on inter-modal interfaces (e.g. parking lot reservations).

5.5 Business work by operators, administrators and facilities owners of public transportation and its related or additional services

For rail, bus and truck, ferry as well as air vehicle modes, see ISO 37154, 5.2.5.2, a), b), c) and d).

EXAMPLE QR code identification and authentication work on passenger, delivery items and freight services as well as the operation (e.g. service dispatching), its technical support (e.g. repair records, operation manuals), safety ensuring and information provision in the services.

5.6 Business work by operators, administrators and facilities owners of private transportation and its related or additional services

For the business work and personal-use public transportation, see ISO 37154, 5.2.5.3, a) and b).

EXAMPLE QR code identification and authentication work on vehicle sharing and rental services (e.g. vehicle reservations, rental contracts).

6 QR code identification, authentication and authorization in or for smart transportation

6.1 General

QR codes in or for smart transportation to be used with temporary keys and matching fields work for personal identification and information content authentication, whenever customers and service agents transfer data. Such QR codes enable safe and quick enquiries on transportation and its related or additional services, which are linked to appropriate websites by protecting customers from tricks and information disclosure.

Conventional procedures to secure data transfer require tedious and complex certificates of identification and authentication. Obtaining the certificate takes time and repeated communication bothers customers and service agents in the process. To avoid such disadvantages, QR code identification and authentication in or for smart transportation should have the following characteristics:

— non-centralized, end-to-end data transfer modes;

— public-key cryptography to ensure high efficiency and low-cost data transfer;

— convenience and security;

— online or offline communication;

— tamper-free and non-repudiated data transfer;

— tractable trading.

6.2 QR code identification

QR code identification is applied whenever transferring data in transportation and its related or additional services, in order to identify data senders and recipients. In the services, data are transferred:

— between customers and service agents of operators, administrators or facilities owners;

— between service agents of operators, administrators and facilities owners;

— between customers or service agents of operators, administrators and facilities owners, and settlement organizations.

6.3 QR code authentication

QR code authentication is applied whenever transferring data in transportation and its related or additional services, in order to protect information contents from illegal action. The data are normally transferred between persons, as mentioned in 6.2.

6.4 QR code authorization

6.4.1 General

It is common that customers make reservations for train, bus and ferry rides, flight services as well as hotel and restaurant. QR code authorization is applied in the reservation process. When people (e.g. customers) are identified and information contents (e.g. reservation details) are authenticated with QR codes, their status (e.g. qualification for taking the reserved seat) is authorized. QR codes simplify authorization processes that usually take time in conventional ways, whereas QR code authorization is processed in a short time in smart transportation. QR code authorization also avoids illegal or wrong action that happens in manual processing.

6.4.2 Authorization processes

QR code authorization works with immediate responses to confirm personal status, which is completed by applying QR code identification and authentication. Customer status is authorized in transportation and its related or additional services when validating and verifying their tickets in a station, ferry terminal or airport, passports at passport control and reservation slips at a hotel or restaurant, for example.

In addition, customers can show their qualification for discounts (e.g. students, repeaters, frequent visitors) and fee exemption (e.g. students, elderly, disabled), when booking seats, beds and rooms as well as buying articles. QR code authorization works just like certificates (e.g. driver's license, entry visa, personal health record).

In QR code authorization, personal information (e.g. name, age, registration place, mobile phone number, e-mail address) is stored in a database in advance after encrypting to protect from disclosure.

6.5 Other practically useful applications of QR codes in transportation and its related or additional services

6.5.1 General

Virtual QR codes can show the latest version of QR code formations, which are not permanently indicated but temporally created for indication on smartphones or at websites. Virtual QR codes should be managed:

— to have authenticity;

— to avoid virus software infection;

— to avoid linkage to phishing websites;

— to validate website domain names;

— to validate website domain spatial.

6.6 Application to data transfer validation

QR codes can work in a limited number of times or no limitation of the number for:

— one-time-only use tickets;

— genuineness of certificate (e.g. tourist souvenirs, packages);

— money receipts (e.g. merchants, shops, restaurants);

— payment (e.g. personal, by companies);

— facility information authorization (e.g. merchants, hotels, restaurants);

— customer status authorization (e.g. right ticket holders, right reservation-making customers);

— personal identification or authorization;

— information content authentication;

— reservations and checking-in and out (e.g. trains, buses, ferries, flights, hotels);

— enquiry links to agencies' official websites (e.g. railroads, airlines, hotels, visitor information centres);

— season tickets (e.g. monthly, seasonal, annual);

— discount coupons (e.g. 11 times, flat rate fare, limited fare and fee values).

7 Security of smart transportation with QR code identification and authentication

7.1 General

In transportation and its related or additional services where operation should be carried out on time, no delay in data transfer is allowed. QR code identification and authentication should satisfy the following requirements:

— the process (e.g. mutual identification) should be completed in less than 200 ms right after reading QR codes;

— both identified and authenticated communication should be protected from risks (e.g. modification, access, blocking, destruction, technological vulnerability).

Security is the most important procedure in smart transportation. At a minimum, QR code identification and authentication security should provide the following for data transfer:

— fluidity;

— controllable anonymity;

— non-forgery;

— non-repeatable data transfer;

— non-repudiation.

7.2 QR code identification and authentication security

In smart transportation by d-payment designated in ISO 37165 where high security is required for money transaction, public-key cryptography secures data transfer by using keys and matching fields dynamically or one time for each time. For QR code identification and authentication, such cryptography should be applied for the same level of security.

Both temporary public and private keys should be created by a data sender (e.g. customer) and a recipient (e.g. merchant). Furthermore, to confirm the matching of private and public keys, a temporary matching field should also be created. The sender's private key, created by the sender, and the sender's public key, created by the recipient using a common algorithm, are combined in a temporary matching field also created by the recipient. In the same way, a temporary field is created by the sender in which the recipient's private key, created by the recipient, is combined with the recipient's public key, created by the sender, in the same algorithm. When both combinations in the two fields are successfully matched, they recognize each other with higher accuracy. To obtain the highest security, all personal object data or public and private keys and matching fields should be temporary and used only once. To quickly process the procedure, an agreement on the procedure to use a common algorithm to create temporary keys and fields should be made between the participants in advance.

To be technically correct, private keys are not recognizable to all participants but only to a data sender and a recipient. Therefore, participants can find only public keys when looking for a specified data recipient and a specified sender.

7.3 QR code authorization security

7.3.1 General

As described in 6.4, QR code authorization is completed by identifying person who is going to transfer data and authenticating information contents, in order to confirm the status of the person. To identify persons acting in data transfer, their personal information is collected in advance and encrypted to protect from disclosure while stored.

7.3.2 Personal information collection and encryptions

Collected personal information, including QR code user's name, age, registration place, mobile phone number, e-mail address and so on, should be stored in a database after encrypting with asymmetric public keys and engaging to an encrypted tag. The encrypted tag works as a label of a data set of personal information.

7.3.3 Security procedures

QR code authorization is secured by following proper procedure. As mentioned in 7.3.1, authorization is completed by QR code identification and authentication where public and private keys to be matched are used.

Customers, who have an identity QR code and whose personal information is safely stored with an encrypted tag in a database, show their identity QR code to a service agent (e.g. immigration officers at passport control, receptionists in a hotel or restaurant). The service agent reads QR code containing the customer's identity encrypted with a private key and sends the identity to the database to identify the customer.

The database can determine a customer's tag encrypted with another private key that is engaged to each customer's personal information. The database tries to combine tag's private key and the private key encrypting that customer's identity in a matching field that is also encrypted with a public key.

If the two private keys are successfully matched with the public key, the database positively responds to the service agent. If not, the database responds negatively.

Upon receipt by the service agent of the response from the database, customers are identified and their status is authorized.

As described in 7.2, private and public keys and matching fields are dynamically or one time for each time used even in QR code authorization. Private keys are also not recognizable to all participants except a data sender and a recipient.

8 Organization and operation of smart transportation with QR code identification and authentication

8.1 General

QR code identification and authentication in transportation and its related or additional services are based on online and offline communication processed safely and quickly with secure-trusted infrastructures.

Mobile data transfer with QR code identification and authentication is useful since smartphones are commonly used everywhere. In smart transportation, mobile phone users can also transfer data with the identification and authentication through mobile communication networks and data platforms or other mobile terminal connections adopted by mobile carriers.

8.2 Secure-trusted infrastructures for QR code identification and authentication

8.2.1 Credible service management modules

Credible service management modules should arrange and manage multiple applications to secure QR code identification and authentication, including access to related business and authorization.

8.2.2 Big data analysis centres

Big data analysis centres should ensure the security of QR code identification and authentication to prevent illegal activities (e.g. fraudulent data transfers, black money laundering, terrorist financing) by

analysing each data transfer communication. Big data analysis centres provide references for the flux and cycle of QR code-identified and authenticated data transfer in smart transportation.

8.2.3 Registration centres

Registration centres should record the following information:

— corresponding relationships between QR code-identified and authenticated data transfer or QR code authorization and user identity information;

— flow of QR code-identified and authenticated data transfer.

Registration centres also complete the registration of data transfer processes with QR code identification and authentication.

8.2.4 Data transfer modules

Data transfer modules should support data senders and recipients to transfer QR code-identified and authenticated data and obtain authorization both online (e.g. internet) and offline (e.g. NFC, bluetooth).

8.2.5 Terminal application modules

Terminal application modules should include mobile terminals that work as modules for client management and terminal security. Mobile terminals are held by data senders (e.g. customers) and recipients (e.g. business operators).

9 Quality maintenance of smart transportation with QR code identification and authentication

9.1 General

To maintain smart transportation with QR code identification and authentication, observe the parameters in 9.2 regularly and make corresponding evaluations to improve the quality of the smart transportation services. This will assist with the planning and implementation of QR code identification and authentication in other geographical areas or business fields in the future.

9.2 Parameters to be observed

The following parameters can be used to compare smart transportation performance. Use appropriate units for observation:

— number of times that QR code identification and authentication are chosen when data are transferred in transportation and its related or additional services;

— time duration spent for data transfer with QR code identification and authentication;

— security verification number taken in data transfer with QR code identification and authentication;

— security verification time duration taken in data transfer with QR code identification and authentication;

— number of agencies and business activities using data transfer with QR code identification and authentication (e.g. per month);

— measures provided by agencies and in business activities using data transfer with QR code identification and authentication in order to protect users' privacy from disclosure;

— QR code identification and authentication introduction or application ratio in target cities or regions where smart transportation is installed;

