TECHNICAL REPORT

ISO/TR 20526

First edition
2017-07

Account-based ticketing state of the art report

Rapport de l'état de la technique concernant la billettique centrée sur le compte usager

Reference number
ISO/TR 20526:2017(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
www.iso.org

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

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

Introduction

Account-based ticketing (ABT) is a subject of wide interest. It is used and is being considered for use by many transport operators and authorities across the world. The system supplier market is international. There may be benefits to transport operators and authorities from some element of international standardization. There may also be benefits from some overall international coordination, for example, with regard to reference data.

ABT is a method of ticketing where the proof of entitlement to travel and any records of travel are held in an ABT back office and not in any physical media held by the passenger. ABT is also known as server-based ticketing or Security in System. ABT can operate in both an online and offline world using risk-managed revenue protection techniques as appropriate.

ABT is widely used for long-distance ticketing such as coach, rail and airlines and there are field deployments of ABT systems in urban ticketing associated, for example, with usage-based best-value tariffs. Although an account is always technically required, entirely anonymous travel is possible and accounts do not need to persist after travel, save for fiscal reasons.

Concepts for implementation of ABT

There are several concepts for the implementation of ABT which have quite different characteristics and value propositions for the public transport operator. The following examples demonstrate this variety.

a) Token authentication by the reader

There are several field deployments of classical interoperable fare management systems (IFMS) systems where the customer's fare media is used as authenticator/token but not for storing fare products. In these known cases, the authentication is done by the readers which have to be equipped with the credentials needed to perform the token authentication. The reader will need then to connect to the account server or to hold a list of authorized accounts before validating access to the user. The implementation follows the role model as given in ISO 24014-1. The customer's account is hosted by the product retailer, who is the only financial interface between the customer and the other roles in ISO 24014's model. In this concept, the payment provider is just a subordinate role to the product retailer and has no relevant influence on the processes and technologies of the fare management system.

Strengths: These systems are also able to perform the authentication also if the reader is offline. The security level may support high-value products and the vulnerability to denial of service attacks is low.

Weaknesses: These concepts support typically the fare media which are explicitly released by the system owner. Use of third-party media [offering the passenger a bring-your-own-device (BYOD) facility] may require integration of the authentication methods defined by the third-party media or application issuer.

b) Token authentication by the account server

This concept is known from access or ticketing systems where a high-performance online connection to the account server is provided. The authentication of the token is performed directly between online server and media. The reader is just transparent or not even necessary if the media is equipped with an online connection like in the case of a mobile phone. The systems can be established based on the ISO 24014-1 role model as described in Concept 1.

Strengths: The concept is very cost efficient and flexible because security functions and credentials are only necessary in the central online server. This reduces cost for the reader infrastructure dramatically and provides the flexibility for the introduction of new types of media. If this concept is combined with the use of asymmetric cryptography (in order to avoid the need to distribute cryptographic secrets to external media providers), the introduction of third-party media is a practical option.

Weaknesses: The concept will not work at all if the media is not connected to the online server and/or performance is worse than authentication by a local reader. However, with improving connectivity and performance of servers and connections, it may become practical in classical fare management environments. If so, it will probably be the most efficient and future-proof way to implement ABT.

Today, concepts are evolving that try to get as close as possible to example 2 (token authentication by the account server) by implementing list-based risk management where truly online connections are not supported. The feasibility for specific fare management systems is subject to an individual risk assessment.

Use of third-party media

An increasing number of fare management deployments are using third-party media for account-based ticketing. This development is driven by contactless payment cards and government-issued cards which are becoming common globally. In addition, where there is use in one ABT scheme of media issued by an external transport organization not involved in the scheme, this also can be seen as third-party media as it generates similar requirements as non-transport third party-issued media.

The payment networks deployed strict technical and certification requirements to their reader infrastructure in order to achieve global interoperability. The ISO 24014-1 role model has to be extended to ensure cooperation with the payment card issuers as identity providers and as payment providers.

Strengths: The public transport service provider can rely on third party media and does not have to equip customers who have their own media. For payment cards branded from the major payment networks, interoperability across ABT systems can be achieved. In this way, even foreign visitors can use their contactless payment card to obtain a public transport service.

Weaknesses: Existing public transport contactless infrastructures need to be replaced or adapted in order to fulfil the requirements of third-party media suppliers, particularly the payment networks.

Real-world implementations typically use classical contactless fare media and contactless payment cards in parallel. Certain categories of customers like season cardholders or unbanked people may be served by fare media issued by the public transport service provider. In an ABT scheme, the implementation of the public transport system owner's internal processes is typically still based on the role model from ISO 24014-1. An example is that of the product owner (which is a role in ISO 24014-1) that calculates fares for all customers including those with contactless payment cards.

Therefore, there is a need to make sure that IFMS concepts defined in ISO 24014-1 can coexist with concepts based on contactless payment and other third-party media. This requires an eventual integration of the role models and a harmonization of the technical requirements, as well as related testing and certification of the reader infrastructure.

Account-based ticketing state of the art report

1 Scope

This document provides a state of the art of the components that make up account-based ticketing as currently understood. This state of the art can be used to identify those aspects where international standardization or coordination can lead to benefits. These will then be proposed as normal ISO work items, independent of this document.

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 terminological databases for use in standardization at the following addresses:

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

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

3.1
access control
control of access to a means of transport, e.g. gates or check-in

Note 1 to entry: See also *ticket control* (3.10).

3.2
card-centric
where the travel contract is represented by data in the media

Note 1 to entry: See also *server-centric* (3.8).

3.3
credentials
elements that provide secure access to the data in media

Note 1 to entry: Credentials will include keys and cryptographic methods used to encrypt or digitally seal the data.

3.4
EMV
Europay MasterCard Visa standards for payment cards

3.5
media
machine-readable device able to store data

3.6
Near Field Communications
NFC
radio communications interface defined by the NFC Forum and largely interoperable with ISO/IEC 14443 and ISO/IEC 18092

3.7
revenue protection
business processes established to minimize ticket fraud

3.8
server-centric
where the travel contract is represented by data in the back office

Note 1 to entry: See also *card-centric* (3.2).

3.9
tap
presenting media to readers to identify the passenger itinerary

Note 1 to entry: The reader reads the token held in the media.

3.10
ticket control
checking a ticket or a token for revenue protection purposes

Note 1 to entry: See also *access control* (3.1).

3.11
token
secure machine-readable instantiation in media of an identity

3.12
tokenization
secure process of substituting a sensitive data element with a non-sensitive equivalent, used in the creation of a token

3.13
usage-based products
transport contracts where the calculation of price is made after travel

4 Conformance

Not applicable to this document.

5 Symbols and abbreviated terms

ABT	account-based ticketing
AFC	automated fare collection
PAN	primary account number
BLE	bluetooth low energy
PAYG	pay as you go
PCI-DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information

6 How does account-based ticketing work

6.1 Business roles

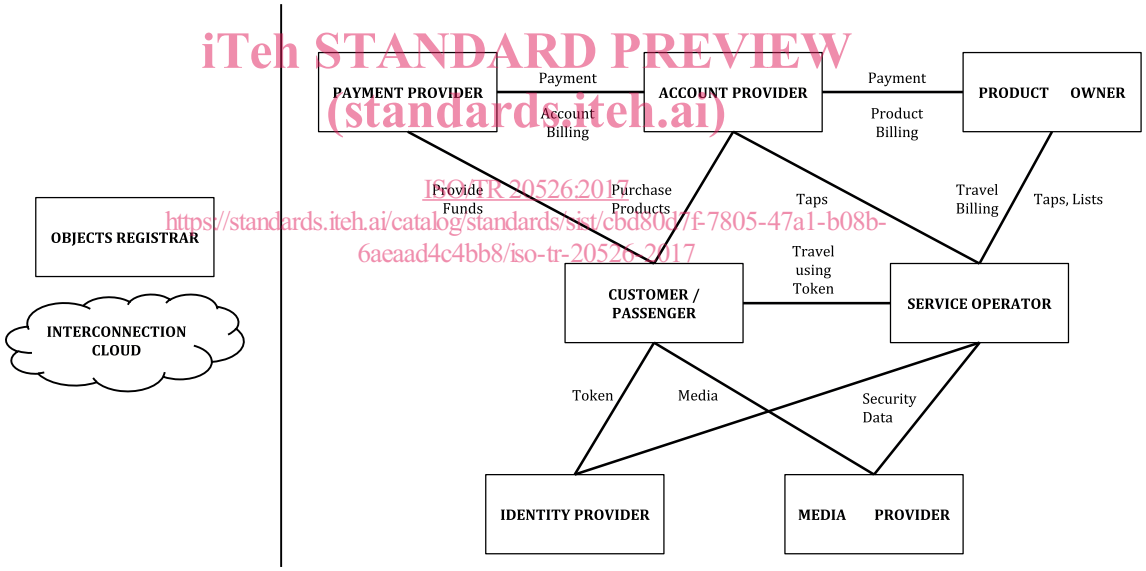
An important objective of this document is to identify the need for update or extension of existing technical specifications and standards or the development of new ones.

ABT concepts include new functionalities in addition to those based on the established ISO 24014-1 model. These concepts lead to the identification of significant new roles that support these new functionalities and may require the combination of functionalities of the new roles and IFM-roles in ISO 24014-1.

There are several ABT schemes in operation today based on IFMs which are compliant with ISO 24014-1. These schemes serve as practical examples of the coexistence of account-based and media-centric system concepts.

The new roles identified in this document should be mapped to those in the ISO 24014 series, together with those coming from the other technical reports that have addressed various developments in IFM systems. It is essential to maintain a practical basis for the seamless implementation of media-centric, back-office-centric/account-based and hybrid solutions based on the ISO 24014 series.

The following business role model is described to suit this objective and should be used as input for a revision of ISO 24014.



6.1.1 Customer

There is a difference between a Customer and a Passenger. The Passenger travels and has entitlements. The Customer has the commercial relationship with the Account Provider (as Product Retailer) and is responsible for payment using a Payment Provider. The role diagram above combines the two roles for simplification.

The Customer can hold one or more accounts. Each Customer holds transport products in the account that are purchased from the Account Provider as an agent of the Product Owner. Each account is associated with one or more active tokens, although the associated media can be changed on the fly if the original token used for a product is lost or damaged. Accounts can be explicitly opened by the Customer or can be implicitly opened on first sight of a token.

The set of tokens that a Passenger may use with a product is set by the Product Owner in agreement primarily with Service Operator. The Passenger should make sure that s/he has the correct token for the product.

The Passenger travels using the products in the account and uses the token on the media for access control and ticket control. The Customer pays the Account Provider for travel according to the rules of the contracted products. The Customer and Passenger can expect to receive support from the Account Provider, the Service Operator and the Payment Provider.

Where the token is associated with a payment account, for example, with payment cards, suitable usage-based products can be automatically added to the account on first sight of the token.

6.1.2 Media Provider

Media in the ABT context is a physical support containing a machine-readable/writable data/processor application. This can include transport industry smartcards, payment industry contactless cards, public sector issued cards, mobile phones or paper (for barcodes), new formats such as watches and key fobs, plus NFC mobiles.

Media Providers can be not only transport authorities and service operators, but also non-transport organizations such as governments central and local, mobile handset vendors and banks.

The Media Provider is responsible for managing all the pre-issuance production processes culminating in media personalized for a Passenger or supplied anonymously. The Media Provider is also responsible for many post-issuance processes, including final decommissioning.

The Media Provider is responsible for the security method employed by the media and for ensuring that the Service Operator equipment is provided with the relevant media security credentials, methods and keys. In the ABT world, unlike the card-centric world, only the Service Operator needs to participate in the Media Provider's security scheme as only the Service Operator has the equipment that is used to read the Customer's media.

6.1.3 Identity Provider

The Identity Provider creates and provides a token that can be trusted to be associated with a Passenger. Product Owners and Service Operators will use this trust relationship as the basis for authenticating the Passenger. Identify Providers can be not only transport authorities and service operators, but also non-transport organizations such as governments central and local, mobile network operators, online service providers (e.g. Google, Facebook) and banks. It may provide to the Account Provider a validation service that can be used to check the validity of the token and all processes for customer support like for trustworthy registration, blocking in case of loss or theft, revocation or re-issuing.

The token used in ABT is a secure instantiation of a trusted identity stored on a media. In some cases, the token and the media are provided together at personalization, for example, with a contactless payment card. In others, the token can be supplied later for storage on the media. An anonymous token can also be supplied for use by passengers concerned about their privacy.

The Identity Provider is responsible for the provision and maintenance of tokens that can be related to a specific Passenger (where a non-anonymous ID is required). An Identity Provider may also provide trusted details of entitlements linked to the Passenger. A secure but anonymous identity can be provided in the case where anonymous travel is permitted.

The Identity Provider may be responsible for the security method employed for identity tokenization and if so, for ensuring that the Service Operator equipment is provided with the relevant security credentials, methods and keys. In the ABT world, only the Service Operator needs to participate in the Identify Provider's security scheme as only the Service Operator has equipment that is used to read the Customer's token. It is common practice that the Identity Provider provides a token (e.g. as certificate) which is stored in a specific token application which come from an Application Provider for eID.

6.1.4 Service Operator

The Service Operator is responsible for providing the transport service to the Passenger.

