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

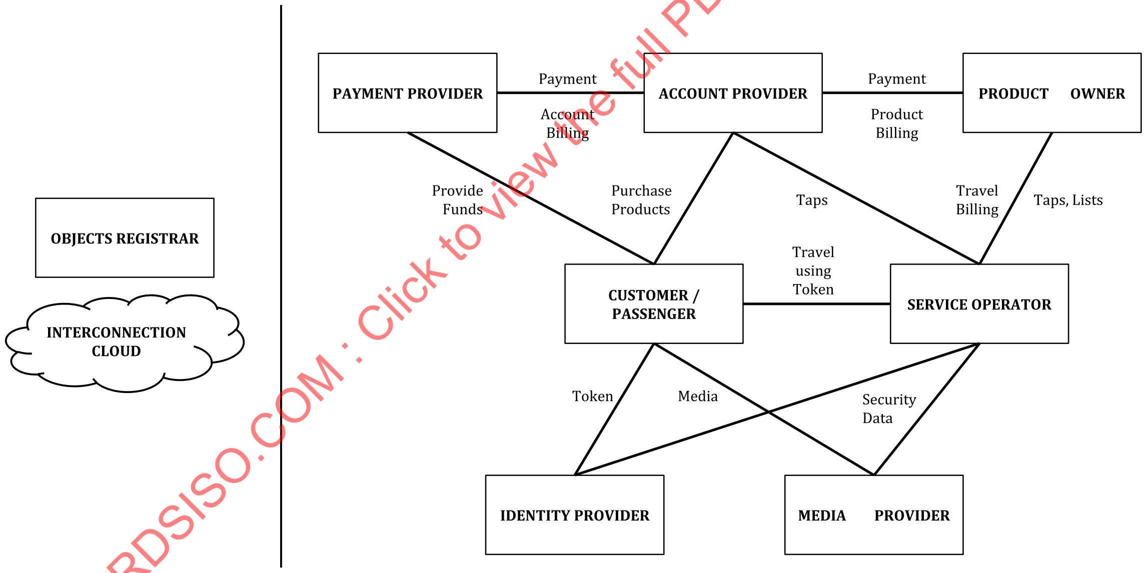
An important objective of this document is to identify the need for update or extension of existing technical specifications and standards or the development of new ones.

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.

The Service Operator contracts with Product Owners for the right to sell transport products. These contracts define the travel services to be provided, the prices and conditions of carriage and the tokens and media that can be used for travel.

The Service Operator is sent Deny and Accept lists by the Product Owner and ensures that these are used by access control equipment and ticket control staff.

Taps will be generated from access control and ticket control processes depending upon the fare calculation rules defined by the Product Owner. The Service Operator sends the taps to the Product Owner, although in some cases, related to usage-based travel, it may be efficient to additionally forward the tap to the Account Provider. This is the only party able to correctly determine the best product for the Passenger to use. For example, the customer may have purchased a long-distance product that includes travel across a city. The Product Owner may not know this explicitly and raise a charge to the Account Provider for the cross-city travel. If the Account Provider received the taps, it would be able to advise the Product Owner not to raise a charge (that had subsequently to be backed out).

Rules are needed in the ABT scheme to accommodate late and missing taps.

The Passenger travels using a suitable token as defined by the Product Owner. Taps on reader equipment or other checks of the token are sent to the Product Owner or Account Provider who selects the best product for the travel undertaken and if necessary calculates the price. Each tap contains information of the token, service and the reader equipment. It can also contain additional other specific information such as the time and location of the tap.

The Service Operator receives payment from the Product Owner for the travel provided.

6.1.5 Product Owner

The Product Owner specifies products based on travel services provided by Service Operators. The definition of a product includes the specific travel service, pricing, billing and clearing rules, acceptable tokens, conditions of carriage, conditions of sale, etc. A Product Owner contracts with an Account Provider to sell their products to Customers. Product Owners will know which of their products an Account Provider has sold and to whom but will not know all the products held by each Customer.

Product Owners reimburse Service Operators for the journeys travelled with one of their products and settle the money with Account Providers for the product instances sold and changed.

Account-based ticketing supports conventional tickets bought in advance together with usage-based products with the price calculated after travel, either using payment on entry or payment based on the itinerary. Where not banned for regulatory or safety reasons, passengers should be able to travel anonymously. ABT products that support this requirement can be provided.

Some forms of travel, such as in groups, do not sit well with ABT, as there can be significant effort to associate the tokens of all the travellers to the group transport product. For this and similar cases, it can be expected that there will always be a residual level of conventional ticketing even if regular travel is priced using a usage-based method.

6.1.6 Account Provider

The Account Provider in this model includes the role of the Product Retailer and has the commercial relationship with the Customer. The Account Provider role can also include that of Technical Distributor (as used in the rail and air businesses). The role model in this document is therefore a simplification of a complete role model such as required for interface development.

The Account Provider sells products as an agent of a Product Owner. Products are sold to Customers. Products can include conventional tickets booked in advance of travel- or usage-based products. For all product types, payment from the Customer can be before travel or after travel, based on the requirements of the Product Owner and the credit-worthiness of the Customer as assessed by the Account Provider.

Products can be sold to anonymous Customers as long as there is a link to a Payment Provider. In order to provide entire anonymity, ABT requires that for all usage-based products, there should be a Payment Provider role that accepts cash and an Identity Provider that can provide an anonymous token.

ABT allows accounts to be created before travel, where the link to the Payment Provider is established in advance, but also upon travel, where the token used should provide a trusted link to an active account held by a Payment Provider.

Where an Account Provider sells a usage-based product, it is necessary for the Account Provider to know of all the other relevant products held by the Customer and their product usage, even in principle held by other Account Providers, in order that the Account Provider can determine from the Passenger's itinerary (as evidenced by the taps) the extent of travel not covered by conventional products which is therefore to be charged to the usage-based product. There is an issue where Customers hold usage-based products that overlap geographically as this can lead to ambiguity over which product is used in which case. The sharing of product information and the best party to calculate the price of usage-based travel products, as identified above for the benefit of the Customer, is a complex subject not yet fully addressed or resolved.

Account Providers will ensure that Customers can create and manage their accounts, verify the authenticity of the presented identities and entitlements, verify the authenticity and integrity of the transactions between Customers and Service Operators, protect the privacy of the customers and service providers, and allow Customers to configure their digital identity including the registration of tokens and the purchase of products.

In the case of usage-based products, Account Providers will receive notifications of product use and cost from Product Owners, provide the Customer with an overview of all services that they have consumed and the associated costs and (together with Product Owners in a manner not yet fully addressed or resolved) manage the Accept list and Deny list for all the tokens of all their customers.

The Account Provider will inform Product Owners of the usage of their products and through Product Owners reimburse Service Operators for the journeys travelled, both conventional and usage-based.

6.1.7 Payment Provider

A Payment Provider is the party that provides funds for travel and particularly usage-based travel. This can, for example, be a bank account accessed by direct debit or credit transfer, a payment card account accessed through an acquirer, a transport purse held by a transport authority or a mobile network operator.

Each product will be associated with one or more Payment Providers and the Customer will choose one best suited for his/her purposes. The Account Provider makes payment requests to the Payment Provider on the basis of the travel consumed by the Passenger. The funds received are passed, subject to commission, to the Product Owner.

7 Impact of account-based ticketing

7.1 Benefits of account-based ticketing

7.1.1 General

Account-based ticketing systems are based on a different architecture than legacy media-centric ticketing systems, but once in place, they offer a wide range of benefits as described below.

7.1.2 Issuing media cost reduction

Tokens used in ABT can be hosted in a very large range of customer media and applications: transit contactless cards, paper ticket with barcode, EMV contactless cards, PIV (Personal Identity Verification) cards, mobile application communicating with Bluetooth Low Energy beacons, with barcode readers or via NFC with validators. The trend is often called the Bring Your Own Device (BYOD) philosophy.

Media issuance can be much simpler and cost effective to implement than in media-centric ticketing systems because media will only bear a token that aims to provide a secure identifier.

There is no longer a need for complex card data layouts required to deal with all complex fare structure.

However, tokens should be able to support a strong authentication process. As mentioned before, tokens should be only accepted in the system if they are authenticated.

As a result, the media issuance costs can be reduced compared to media-centric systems.

— Where media has to be provided by a transport service operator or a product owner, passengers can be supplied with smaller capacity smartcards. They only need to hold tokens, which require small memory size.

— Media manufacturers are introducing simpler and cheaper token-only devices into the market.

— Third-party media such as PIV and EMV contactless cards can be easily accepted at no issuance cost for the service operator. This as a result cuts operational costs for the service operator.

7.1.3 Equipment validation simplification

Validation equipment can be much simpler: it does not need to hold transactions for collection, complex fare data nor acceptance rules. Open standards for data exchange between readers and the back office become practicable and an opportunity to break away from supplier tie-in.

The validation equipment's main features then become reduced to the following:

— authenticate the media and its token (locally or via a back office request);

— manage secure communication with back-office to transmit on the fly validation data;

— handle lists of denied and/or accepted tokens to enable offline decision when connection is too slow or not available.

7.1.4 Business rule seamless update

It is no longer a requirement to download all the fare management business rules to the reader equipment. A further advantage of this feature is the possibility to change business rules: changes are immediate (which cannot be the case with media-centric systems) because there is no request to have each piece of equipment to be downloaded with the new version of the application logic implementing the business rules. As a consequence, AFC system operators have a great flexibility in order to change business rules depending upon any event they want to manage. It is emphasized that all existing business rules remain fully applicable. New products based on customer usage can be easily added. It brings a strong customer benefit: users can automatically pay the best fare according to their trips.

7.1.5 Instant product management

Any product purchased by a traveller can be immediately used: the customer account is immediately updated and there is no delay for him to use his/her newly purchased product. Therefore, products can be added, changed and removed easily without being updated by a reader and without changes to the equipment used by the customer to travel.

7.1.6 No media/back office reconciliation

Because all the transactions are managed at the back-office level, there is no longer a need to reconcile the customer media and the image in back office. Customer service and back-office account changes do not require card update and reconciliation.

In addition, passenger usage information is available in nearly real-time, which was never the case in media centric systems.

7.1.7 More flexible customer management

Both anonymous and enrolled customers can be managed in ABT systems just like in media-centric systems. Multiple tokens can be associated with each customer where service operators have different validation equipment.

7.1.8 Improved customer service

ABT simplifies customer service and makes it more efficient.

Tokens can be substituted immediately: there is no longer a need for card reconstruction. This removes the complexity of lost/stolen/bad media and the delays related to that kind of operation: the customer can immediately recover his/her media. It is also no longer necessary to update the back-office card status according to registered transaction because all transactions are only made at back office.

No fulfilment equipment is needed to issue or print or load data on to physical media. This removes the need for customers to go anywhere or do anything to be able to travel on a product, specifically the unhelpful obligation with media-centric technologies to load the product on a smartcard.

Only service operators need to have the security credentials from identity providers and media suppliers. With card-centric technologies, the security credentials are also needed by retailers and fulfillers, adding to costs and risks.

7.1.9 Simpler interoperability

ABT makes simpler interoperability because all information is stored at back office and, therefore, nothing has to be done on the token.

7.1.10 Faster time to market for new technology evolution

ABT system allows easier evolution when technology evolves. Therefore, the consumer market can interact more quickly with the ticketing system and promote ticketing system usage.

7.2 Disadvantages of account-based ticketing

7.2.1 General

Setting up, operating and updating an ABT system has a cost. System operators should be aware that while there are indeed possible cost reductions as indicated in the previous subclause, there are also new costs, and that both should be assessed. The main disadvantages inducing new costs are listed hereafter, equally with some already identified mitigation recommendations.

7.2.2 Keeping the front-office equipment connected to the back office

Transaction processing changes from end-of-shift/traffic day processing to continuous triggers based on tap receipt. This is more susceptible to ICT service interruption.

Front-office equipment has to be connected permanently to the AFC system back office in order to ensure all the authentication and/or validation collection processing. When this connection is not available, risk models apply which are described in 8.1. Therefore, it imposes for the service operator to use a network which has a very high reliability and a high availability level.

7.2.3 Treating transactions upload as business critical

The process for uploading transaction from front-office equipment to the back office is more sensitive than in media-centric systems, which generally used prepaid products and in which validation data are mainly uploaded for statistical usage.

In ABT system, the loss of validation transactions may imply some loss of revenues. It is therefore important to make sure that the uploading process is reliable, periodically done if not achieved in real time and secured with retry/anti-replay mechanisms, as well as non-repudiation processes to offer some resilient means of collecting transactions and, in consequence, revenues.

7.2.4 Minimizing transaction speed

In urban public transport, customer flow is a key operational and safety issue. Therefore, reader transaction times should be as fast as possible. Therefore, communication and processing at the back office should also be at very high speed to ensure full processing of the transaction in a limited time. In case of transaction time exceeding this maximum allowed time, the customer may be authorized by default to enter the system. In this case, risk management processes are applied to maximize revenue to the service operator. In normal conditions, the customer will be authorized to enter the system only when the token has been authenticated.

7.2.5 Supporting multiple technologies within the front office equipment

In order to accept a wide range of tokens, the reading equipment should be adapted to manage them. Therefore, they should include in the reader software all communication software stacks and related security authentication processes for each token type to guarantee that the transactions are properly completed.

This may add to the cost of front-office equipment if contactless, barcode or BLE technologies are to be supported, or if several types of authentication processes are to be implemented in the front-office equipment when performed locally.

However, there is a move from bespoke equipment to consumer products which makes the support of multiple technologies not necessarily so expensive to integrate.

7.2.6 Making AFC back office able to support third-party technology and authentication

In addition to its own equipment, the AFC back-office system should be able to manage data coming from different sources in order to authenticate them and to process them in the requested way. The management of PIV or ID card certificates and security features are critical, plus connection to third-party systems that will provide the authentication services.

7.2.7 Performing control on read-only media

It is not possible to write on most of the third-party media such as contactless payment cards. This creates new constraints for inspection process as no event or history of usage will be available when reading the media.

This requires to retrieve validation information directly from the on-board front-office equipment or from the back-office system. In this respect, revenue control process has to be completely rethought and triggers revenues risks that should be assessed.

However, revenue risks generally are acceptable in urban areas where the single trip cost is small.

7.2.8 Building and maintaining customers' confidence

Customers need to trust that the account provider and the product owner are providing the best value tariff when using usage-based products — trust in commercial entities is easily lost.

Communication will be fundamental to build this trusted relationship even if service operators are generally seen as trusted companies. Communication should rely on information via web or mobile application allowing real-time follow up by the users. It may also rely on communication campaigns towards visitors and tourists in the stations, in the vehicles and through digital media to explain clearly to them the mechanism and benefit of PAYG and/or related capped fare policy. Examples of this already exist in current usage-based ABT schemes.

8 What are the significant features of account-based ticketing?

8.1 Revenue protection and journey recording

8.1.1 Purpose of recording journeys

For usage-based products, ABT (and card-based concepts) use recorded waypoints ("taps") along a journey to determine the subsequent fares or charges to be applied for that customer. Taps may take the form of active presentations of a passive token (for example, a contactless card) or an active device (for example, a mobile handset). Each tap is required to provide sufficient contextual information to permit the subsequent Service Operator to determine the respective fare to be charged. Typically, this will include the date, time and location that the customer token was recorded. The location may include the specific device used, the station/stop/bus details, etc. More sophisticated systems may include the operating mode of the device that was used, or the prevailing operating conditions of the location (station) at that time, such that emergency conditions may be accounted for. The purpose of the data is to enable the intended journey of the passenger to be recreated from the evidence generated along that journey.

8.1.2 Common approaches and typical data flows

Tap data is reported to the back office for journey reconstruction and charging purposes. Two primary approaches have evolved to accommodate ABTs:

- online back office checking;
- pseudo-real time tap reporting.

Online back-office checks are performed where the device is able to reliably query the back office in real time during the validation of the customer's token. The back office is able to utilize the latest risk checking information (current balance, account status, etc.) to determine if the customer should be permitted to travel and to notify the validation device directly via a request/reply message sequence. Online back-office checks are typically utilized where the system supports a prepaid usage-based account. To handle those occasions where the back office may be unable to satisfy specific transaction timing criteria, the device may fall back to a historical status of a token in order to make a local decision. This historical status may be determined by the absence (or presence) of a given token on a Deny (or Accept) list which is periodically refreshed by the back office. The frequency of the refresh and the total size of the list which may be accommodated by the system/reader will determine the level of fraud protection which may be provided. The effectiveness of this method also depends on the reliability and availability of communications connectivity.

Pseudo-real time tap reporting provides a fall-back to being able to support real-time checks against the back office. Rather than query the back office directly, this method transmits the transactions to the back office in slower time, with the transactions being processed on receipt at the back office and the response being represented through Accept/Deny list updates as required. This method may be preferred for the upgrade of legacy systems to facilitate a lower-impact route to supporting ABT functionality. It may also be used in conjunction with the online checks where the online query was not possible.

Note that some systems may choose to differentiate the messaging on the displays to enable (primarily) staff to know when the response is generated locally or whether it has successfully reported from the back office.

Be-In/Be-Out (BIBO) and Check-In/Be-Out (CiBo) systems are now increasingly harnessing the capabilities and ubiquity of mobile smartphones to provide customers with flexible mobile ticketing options. Such devices utilize the built-in communications capabilities to report location and customer/token ID. During the exchange, the smart ticketing app will typically query the back-office server directly to determine if the device/customer is still registered, has a valid means of payment, etc.

8.1.3 Functional operations at infrastructure to record journeys

According to 8.1.2, Check-In (and Check-Out) validation devices will typically follow the following sequence of activities:

a) identify the token medium being presented;

b) read and authenticate the token credentials from the medium;

c) depending on the architecture, request an online query for that token identifier;

d) check for the presence (absence) of the token identifier on a Deny or Accept list;

e) permit passage if permitted;

f) generate a tap record to report the activity performed.

The range of customer media that may be accepted for use is therefore dependent on the level of protection which may be afforded by the inherent security associated with the production of that medium. For example, barcodes may provide greater flexibility in data attributes held and utilize public key encryption to ensure authenticity, but this may not prevent against the creation of multiple copies of that barcode. Bank-issued contactless cards may prevent cloning, but the performance and issuance of these cards are outside of the transit agency's control.

8.1.4 Controlling fraud

The control of ABT fraud during access control or ticket control is based primarily on lists — Accept lists that indicate that a token may be accepted and Deny lists that indicate that a token will be rejected. Other lists may also be used if required by the scheme, for example, to update the token data in some manner, but the conventional use of action lists to load travel products is not required. In ABT, the reader does not normally write anything to the media.

Revenue protection mechanisms typically include the use of Accept/Deny listing to control the acceptance of tokens in the system, as detailed in 8.3. These lists are constructed and maintained by the back office based on observed travel and account behaviour. As with traditional card-based systems, the fraud rules will seek to identify abnormal travel patterns (for example, perceived concurrent travel with multiple tokens), or continued undesirable behaviours (uncompleted journeys or long-term debt).

To supplement these controls, additional risk management capabilities may be introduced to support contactless payment card usage. These rules can seek to balance the number of authorization requests submitted (and for which payment is made) versus the degree of travel permitted on unauthorized cards. The complexity of these rules may take into account the long-term history of that cardholder, rather than focusing purely on the day-to-day usage to recognize that customers build relationships with the transport operator over time.

8.1.5 Implications for inspection

The system readers will validate tokens as they are detected, in accordance with the prevailing authentication mechanisms for that token type. Tokens used for travel are typically passive and will not be modified during the presentation process, apart perhaps from data generated by the authentication process. One exception is for contactless payment cards, which utilize internal risk management methods to control offline usage and to cryptographically sign any tap data which is generated to confirm to the issuing bank that the card was present (in the future, these cards may also store data locally). Consequently, to determine the current status of a given account and associated travel token, it is necessary to adopt an alternative approach to that used by card-based systems.

In general, all usage taps will be received from the devices within the system at the back office. However, due to real-world implementation constraints such as communications issues and outages, transaction processing batching, etc., it is not possible to guarantee that the back office holds the latest up-to-date usage status of a given token. As with validation devices, it is possible that Accept and Deny lists can be distributed throughout the system to allow some degree of offline revenue protection operation, but these are similarly subject to lag time in refreshes. Where such information cannot be ascertained from a more immediate local source (such as a station-based caching system), then a more radical solution is needed. Consequently, revenue protection policies may need to adopt an alternative approach.

In those scenarios where guaranteeing the token status is not possible, ABT systems to date have opted to utilize the inspection process as a means to gather an additional tap. This tap signifies that the customer was being inspected and that tap can be used as a means to charge a penalty[1] fee where during subsequent fare processing, no prior journey starting tap can be located. This is a more passive non-confrontational approach than is normally used for revenue protection.

In contrast to the general case above, inspections on a given vehicle may be simplified where all customers on that vehicle should have validated on-board. Consequently, by retaining a record for the duration of a given trip, a local record that identifies those tokens that were presented should exist. Depending on the form of the token(s) used, that list may take the form of a printed list, or an electronic manifest which is transferred to a given inspection device. This list can then be referenced. Depending on the nature of the interaction, it is also possible to use the presentation of the (unvalidated) token to trigger the charging of a penalty fare as per the off-vehicle case.

8.1.6 List management

8.1.6.1 General

As per the above, lists may be used to both improve the customer experience and to supplement the fraud management operations where communications connectivity is not possible. Such lists are typically utilized as follows.

8.1.6.2 Accept list

This is used to identify those tokens which are acceptable for use in the system. This may include those customers who have pre-purchased a conventional ticket product, registered their details to use the ABT system, provided payment details, or having established a positive PAYG credit balance. Tokens are removed from this list as they are subsequently deemed unacceptable (e.g. ticket used, payment subsequently denied, bad debt risk, token lost/stolen). Note that where multiple tokens are permitted against a single account, this list may hold some tokens (for example, those not lost or inactive) or no tokens (for example, where the customer is a bad debt risk).

8.1.6.3 Deny list

This is used to identify those self-issued tokens which are not acceptable for use in the system. This list will contain those tokens which have been lost or stolen since issuance or which should no longer be permitted for travel due to lack of funds and/or acceptable means of payment. The expectation is that the majority of the tokens issued will remain valid. Therefore, this list should represent a subset of the total population.

In each case, utilizing an expiry date within the token will naturally have a culling effect over time. Tokens which are added to the list should remain on the list until they are expired (or until fraud rules

[1] Although the purpose of the fee is to provide a penalty, it may be preferable to consider this as a service fee, published as part of the product tariff rules, to minimize complaints from customers that they have been charged arbitrary amounts in the back office without their express agreement.

deprioritize their inclusion) as typically, there is no way to mark a given token as having been centrally blocked.

Depending on the size of the system, the list sizes may be significant, requiring complex management methods to ensure efficient distribution and updates. This includes the broadcasting of updates and the use of delta lists to frequently make changes during the normal operation of the system. As the level of fraud protection is related to the frequency and accuracy of the lists held in the devices, further complexity may be introduced to target updates to specific locations in order to minimize the time lag involved. For example, list updates following processing of a token at a given station may be scheduled to be distributed to a wider and wider set of stations around that original point of usage as time goes on, or to target known points of usage for that customer first. This minimizes the overall load on the list distribution system and may help increase fraud protection.

The system should be designed to accommodate the bandwidth associated with the maintenance of the lists alongside the normal operation of the system. This includes making provision for list storage and efficient list management and referencing within the validation devices.

Where systems may be aggregated, opportunities exist for sharing Accept and Deny lists as may be undertaken for card-based systems.

8.1.7 Use of media-based data storage other than the token ID

Potential improvements in ABT business processes can be made in the case that additional data can be stored on the media. Examples of this would be a token expiry date created at personalization or at a later stage which would allow the token to be removed from Deny lists once it had expired. Another example would be the storage of some recent transaction data, using concepts such as a card transit data area or a Customer Convenience Register. This data would help for revenue inspection, for example, as an inspector would know directly from the media whether the passenger had checked in. It would also help where a Deny list had been cleared in the back office but not yet on a local gate — the local data could be used to allow entry.

The primary difficulty with local media-based data storage is that it is unlikely to be available on all the media used in an ABT scheme. If revenue protection methods have to be developed to work satisfactorily without local media-based data, then the benefits of including it are much reduced. This balance is something that has to be decided scheme by scheme.

8.2 Data privacy

Tokenization, as used by ABT, provides a method that as a matter of course keeps Personally Identifiable Information (PII) sensitive data away from the client devices to the furthest extent possible. There are, however, additional considerations in the case of transport ticketing.

The first issue is what constitutes PII and, in particular, the distinction between sensitive and non-sensitive PII. The subject is already addressed in ISO/IEC 27018, in the PCI-DSS requirements with regard to payment cards and also in national and regional legislation, for example, Directive 95/46/EC (also known as “Data Protection Directive”) and its proposed replacement. These documents may be relevant in the design of an ABT system. The matter is made more complicated as public opinion towards data privacy varies country to country. The issue is of increasing sensitivity, given the changes in light of exponential growth of data and regular use of personal mobile computing devices. This can lead to de-anonymization/re-identification practices, location and habit-based fingerprinting and combining disparate datasets to defeat anonymity. All of these are relevant in the case of ABT.

Some jurisdictions restrict the geographical usage allowed for a single token. For example, different tokens can be required by law for different types of travel in France. This imposes constraints on the customer/passenger proposition and the options for interoperability.

Although this is a contentious subject, there are no specific ABT data privacy topics that appear suitable for WG8 standardization.

8.3 Options for travel tokens and management of multiple token credentials

8.3.1 Background

ABT can hugely improve seamless usage of transport services by accepting travel tokens from multiple entities — bring your own device. Travel token issuers may include transport operators and authorities, governments, banks and other trusted ID providers.

This goal becomes feasible while moving some elements (e.g. ticketing business rules, also the media data-models) from the devices ("readers" and customer media) to the servers, thus reducing the number of requirements and constraints at media level (data-models and rules).

This opens the door for each ticketing system to accept seamlessly media from other schemas.

However, we have to keep in mind also that some other features usually present on a secured distributed ticketing system also move their "centre of gravity" and need to be studied and standardized. Special examples are the security and the performance of transactions.

Before going into more details, different categories of "ticketing media" normally associated to different technologies are identified:

Static media: Media which only stores static ID, which data never changes. Examples: QR-code, 2Dbarcode, contactless card number, long-range radio frequency tag;

Passive dynamic media: Media which can store dynamic data, which may eventually host some temporary data, even if the "account" is not stored on the media. Examples: transport contactless card from "external" schema, with user-data on a "PayPass Advance" type banking card;

Active dynamic media: Media which, besides the ID and eventually storing some temporary data, has also communication and user-interface capabilities. Examples: NFC/HCE smartphone, NFC/SIM smartphone, BLE (Bluetooth Smart) smartphone operating on a short- or long-distance mode, smartphone using "ultrasonic" tags. Of course, some of these media can also operate in the static and/or passive dynamic mode.

Depending on the media, more than one transaction flow can be used. In the classical paradigm, the reader accepts the media and checks the account on the server (online or offline). The reader is the "active part". This is the classical paradigm, but in which rules and data-models may shift to the server. It typically applies to all three types of media and is compatible with access control systems (but some limitations may apply if rules checking on the server need to be performed online). It also supports the Be-in/Be-out paradigm.

In a new paradigm, the media "accepts the reader" (which in this case can be a "tag") and checks the account on the server. The media is the "active part". This is a new paradigm, because the "reader" can be reduced to a "tag" (or even nothing at all), and rules and data-models may all shift to the server. In addition, communication is performed by the media (e.g. smartphone). Typically, this applies only to active dynamic media and is difficult to use compatibly with access control systems. It also supports Be-in/Be-out paradigm.

Although the classic paradigm is the typical way, in fact, these two paradigms may co-exist, or tend to co-exist, depending on social and economic conditions on each country and region, and therefore the ABT definitions should be able to cope with both.

Nevertheless, for a pure ABT transaction, a "static media ID" should be enough ("ABT-Media").

Also, the compatibility between ABT and classical "stored value media" ticketing (carrying either "conventional ticketing fixed tariffs" or "usage-based ticketing") should be supported, so that barriers to ABT introduction are minimized and application can be performed to specific groups (e.g. higher socio-economic groups, tourism, etc.) without disrupting the mainstream model (e.g. pre-paid and subsidized tickets in gated/closed systems);

Regarding technology (and its interoperability), and for each scenario above, compatibility issues should be ensured between the reader and media:

— “Active Part” hardware/firmware should be prepared to modularly accept: QR-code/2D-barcode, ISO-14443-A/B contactless card, EMV contactless banking card, long distance radio frequency, NFC/HCE, BLE, etc.;

— “Active Part” software embedded architecture should consistently virtualize the means to communicate with different technology in a modular way.

8.3.2 Work to be done

Effort has to be spent on designing a model that brings some sort of consensus or standardization of the security model associated with each token (credentials, keys, at which level of the system security checks are performed), as well as to keep the separation between technology and security, towards allowing that each credential/token to be used throughout different media technologies mentioned above.

Concerning the security model, it is firstly important to define the architecture and flows for online and offline validation. That said, there are several topics to be studied and designed:

a) Media ID tokenization: Modelling and security “ABT-Media IDs” that can be accepted by any validation device, using tokenization methods, independently of the “ABT-Media” being linked to a bank (credit, debit) account or to a close-loop account. Similar tokenization techniques to obscure bank PAN should be applied. This should lead to a 1) common format for tokens and 2) security management schema that supports a minimized number of keys to be stored on the validation devices (especially for the offline validation), since many tokens/IDs will be accepted at each validation device.

b) Validation records: As well as for Media ID tokenization, some design should be done at the level of the storage and security of the resulting transaction records, depending on being online versus offline. PCI-DSS storages mechanisms can be checked in terms of applicability to a scheme.

c) Validation devices: Besides the security mechanisms designed on items 1 and 2, resulting requirements for validation devices should be evaluated, in technical terms and also in economic terms (e.g. evaluating impact on the overall investments and feasibility of large scale migration of existing devices to, for instance, EMV and PCI-DSS level specs).

d) Validation performance: The typical <500ms transaction time[2)] will depend on the transaction being online or offline and on the communication infrastructure. The offline case should be favoured for performance issues and, in this case, additional Deny list formats and management flows should also be designed in a way that it can be sustainable to operate.

It should be noted that under PCI rules, it would not be possible for all schemes to share obfuscation keys and salts used to tokenize payment cards. This means that if schemes wish to exchange obfuscated PANs or tokens, they would need some method to convert tokens from one participant’s keys/format to another. Some form of payment token conversion service would be required for the purpose either as a bi-party, hub or centralized service. When initially designing tokenization methods, it would be valuable to define the token conversion protocols, so that if an exchange approach that requires all bodies to use the same tokenization method was chosen, albeit with different keys or salts, that should be known at the start. If in fact the central sharing/token exchange protocol is able to work via unencrypted PANs, then each implementer would, in theory, have total freedom to use different tokenizing schemes, as long as the exchange system was able to create and output tokens in their chosen format. This token sharing design is a non-trivial design activity and would probably be a task best undertaken in collaboration with card schemes’ transit groups.

Regarding the separation between technology and security, it may be a little facilitated once the complexity of rules and data-models is shifted to the server, so the transaction between the reader and

[2)] This target transaction time is needed to avoid possibly dangerous interruption of passenger flow through gatelines.

the media becomes eventually more similar to a “simpler” authentication transaction (but still keep in mind that a secure transaction may suffer some performance issues if, depending on the schemas, it requires some online check on the account server, especially on gated/access controlled systems).

In summary, if it is true that standardizing a Worldwide or European universal standard for media data-model has been a difficult task, the standardization of ABT may be a “simpler” step, but it needs to address preventively the standardization of a security model, supporting a well-defined set of credential and authentication methods between media and readers (avoiding preferably the need for online communication to the server), while keeping these methods supported independently from the media technology.

8.4 Management of customer accounts with multiple tokens

8.4.1 General

One of the main advantages of account-based systems is that they are independent of the technology employed for the tag. Card-based systems are dependent upon the functional capabilities of a given technology’s characteristics. ABT system architecture is more affected by whether it is fully online or not. Bearing that in mind, ABTs are in general abstracted from the token media employed.

8.4.2 Media technologies

8.4.2.1 Overview

As identified earlier in this document, the media that hold tokens are generally electronically readable to support fast and efficient customer validation, which has typically meant the (re)use of a number of existing formats:

— contactless (ISO/IEC 14443-compliant) cards, fobs or mobile;

— 1D/2D (typical) Barcode (paper, card, mobile);

— Bluetooth Low Energy identifier (active card, mobile).

As noted in Clause 7, one of the goals of ABT is to simplify and standardize the front-end readers, thereby helping to reduce the cost of ownership of this device. To that end, it makes sense to rationalize the number of forms of media which are accepted; however, this is then tempered by the number of corresponding media which may be in the market in a given location.

Utilizing the above technologies, there are then a number of issued media types which may use these technologies. Each of these is required to support a single unique ID to prevent unauthorized changes to the information held (if at all) and to facilitate authentication of the data/ID held.

8.4.2.2 Contactless payment cards

Contactless payment cards and fobs may be issued by third-party banks, or as private brand transit cards. These take the form of credit and debit financial instruments, which are either issued to customers upon meeting eligibility criteria or are purchased as a prepaid product. These media are typically issued on a three-year refresh cycle and adhere to the EMV standards for application processing. Performance is governed by the issuing party based on the chip technology purchased and used in the cards. Issuance is subject to the respective local banking environment, although Global initiatives such as ApplePay have helped to unlock this. It should be noted that Contactless Payment Card usage will require the respective system components to comply with PCI DSS controls.

8.4.2.3 Employee cards

Some large transit operators may opt to allow the use of existing (contactless) staff cards which have been issued for the purpose of access control, time and attendance, etc. to access the transit system. These are issued under the employer’s control but may utilize third-party identification and authentication mechanisms which may introduce information sharing challenges. These cards typically carry photographic ID. Issuance of these cards is subject to the rules of the third party and may not be sufficiently robust to ensure uniqueness.

8.4.2.4 Transit cards

Transit cards may be used in an account-based scheme in two ways: as a token in its own right, or to carry a ticket "product" which can act as a token. When acting as a token, the transit card is effectively a local token under the transit operator's control. Though this may remove some of the benefits associated with defraying the costs of issuance, it retains control on the part of the transit operator while still enabling an account-based system approach to be followed. Account-based "products" represent a potential transition strategy, whereby existing cardholders may be migrated over as they enlist into the ABT programme. In the short term, readers may continue to operate as per normal, with the ABT "product" effectively providing an access-all-areas permit to allow customers to travel.

8.4.2.5 National government- or local government-issued media/ID

In some territories, national or local government may issue electronically readable ID cards, entitlement cards, driving licenses or other forms of credential. It can reasonably be assumed that the credential issuance processes will be as secure and trusted as that for transit media.

8.4.2.6 Identity provider-issued media/ID

Examples of this can be seen with Apple and Google/Android handsets and Passbook-style IDs.

In general, the design of ABT systems will attempt to distil each type of token into a common format for use within the wider system. This has the benefit of preventing the need to redesign significant portions of the system to accommodate a new token technology, or a change to an existing technology. It also ensures commonality in list handling, tap reporting, etc. in order to optimize the use of resources.

8.4.3 Impacts of using third party-issued media

In this context, the third parties are any organization other than the one running the ABT scheme. Typically, this would other service operators, but also non-transport organizations such as governments central and local, mobile handset vendors and banks. There are benefits to accepting third party-issued media:

- issuance costs associated with the purchase, personalization and distribution of cards is defrayed to others;
- support costs, including (card) help line and replacement costs are covered by others;
- the third party is responsible for maintaining the security and performance of the media.

However, there are a number of downsides associated with handing over control to another party:

- security of the cards, from issuance through to cardholder receipt, is outside of your control;
- performance of the cards is outside of your control; the issuer may be less concerned regarding robustness and contactless performance than the transit operator;
- the card refresh cycle may be a lot more frequent than a traditional transit card; this will require customers (or the third party) to notify of such changes, incurring cost;
- the third party may place constraints on the use of their media (for example, a card scheme may be willing to allow their card to be used to travel if that card is to be charged, but not if that card is being used as a token against an account which will seek payment from an account provided by a competing card scheme).