Calypso®

White paper

Account Based Ticketing

with Calypso

BMC MOBIB n.v./s.a.

Calypso Networks Association

RATP SMART SYSTEMS

AUTHOR

Calypso Networks Association

EDITORS[1]

Pierre-Paul Bertieaux,
General Manager,
Mobility Card – BMC

Nicolas Generali,
Technical Manager,
CNA - SNCF

Francis Sykes,
Product & Marketing Director,
RATP Smart Systems

FOREWORD

Account Based Ticketing is already considered as the next major evolution in Ticketing Systems, while Calypso - a card centric model deployed in 125 cities around the world since 20 years, has been adopted in many contactless ticketing schemes in the world.

By combining the two models, CNA truly believes that each network could take advantage of both worlds, regarding their own issues and specificities.

This white paper marks the first step of a Calypso Networks Association initiative, which aims to raise companies' awareness to the benefits and shortcomings of Account Based Ticketing.

Following the publication of this white paper, CNA has launched a working group in June 2017 and a set of guidelines of specifications for an ABT – Calypso system has been released in December 2019. Those guidelines provide a framework to implement an ABT system by taking advantage of the offline capabilities of Calypso in order to mitigate the shortcomings of ABT such as the limitations of telecommunication networks. These guidelines can be downloaded on the Technical Calypso Website and are reserved for CNA members only.

[1] Editors of the first version published in May 2017

TABLE OF CONTENTS

1 CONTEXT

1.1 Purpose and content

This white paper deals with Account-Based Ticketing and Calypso. Calypso was started at a time when telecom networks were notoriously unreliable, which accounts for the fact that it was then deemed indispensable that transactions should focus on the interface between smart media (then only Contactless Smartcards) and terminals. Technologies have matured; networks are becoming more persistent and reliable; open-payment systems are now a reality. In the light of these evolutions, it makes sense to analyse account-based ticketing in conjunction with Calypso to see what part Calypso could and should play and what evolutions are required, if any. This is what this white paper is about.

1.2 Looking-back at card centric approaches

To know where we are going, it is important to analyse where we are coming from.

Initially, tickets were on paper. On this kind of support, there were only passes or counters, punching a hole per journey.

The functionalities were strictly limited to counting the number of journeys. After that, paper tickets with magnetic stripe were introduced. This allowed some additional functionalities via to the capacity to read and write information from /to the magnetic stripe. The major addition was the transfer between vehicles.

By reading and writing information at each validation, transfer rights could be granted automatically based on a set of business rules. By just punching a hole, this was next to impossible. The last evolution was the smart card or smart ticket. The extended memory and processing capability features more functionalities and security.

In the conventional card-centric approach to ticketing, the rights/value that can be used to travel are registered on the card. During the validation process, the validator checks that the card is genuine and that appropriate rights/value are present. The validator consumes the value/rights, updates the data on the card and signals that the transaction is valid. This will translate in sending the appropriate visual/sound signals that can be perceived by travellers + other parties involved (drivers, inspectors etc.) + back to the back-office. In the case of gates, it will actuate the opening of gates. The user will get a positive feedback that the validation has been successful. Conversely if the transaction has not been successful for whatever reason (insufficient credit, pass expired etc.), the user will also be informed either by a negative sound/visual feedback or by the absence of any feedback. This way, on the one hand, the passenger is informed as to the status of the validation and on the other hand, the value on the card has been updated to reflect the trip. This is thanks to the fact that card-terminal transactions are secure and instantaneous. By reading the card, inspectors can check that the card has been validated without requiring accessing the back-office.

The main drawback of card-centric systems is that:

- terminals require a certain level of intelligence and
- the data (whether it be transactions, settings or even embedded software) must be synchronized and managed.

This results in limited flexibility and synchronizing the system is complex.

However, card-centric systems are resilient with respect to network failures.

We will now see how ABT architectures address the limitations of card-centric architectures. We also see that ABT systems have limitations and that Calypso can play a part in addressing these limitations.

1.3 Definitions

When referring to account-based ticketing, many terms are often used. Here are a few definitions.

Account-based Ticketing systems

Also known as ID-centric, Server-centric, Cloud-based, Server-based (ISO name) or Security in System (ISO name). These terms refer to systems where the processing takes place in back-office and where cards/POs are used merely for securely identifying holders and linking them to accounts.

Open Payment

Also referred to as open-loop payment, it refers to schemes where acquirers and issuers differ.

Open-loop payments networks operate via a system that connects issuers on the one hand with acquirers on the other hand. Well known open-loop payment schemes include the likes of Visa and Mastercard which do not issue cards directly but brand cards issued by banks.

Pay-as-you-Go

Pay-as-you-Go is an expression used for various kinds of services, from tax to telecom including transport. In transport systems, this expression is used for value contracts. It can be an ABT or a card-based value contract. This works mainly with pre-paid approach. An amount of money is loaded on a card or on an account. It may stay anonymous. The only information required is the link between the wallet and the account/card.

Each time the card is validated , an amount is debited from the card. It can potentially be used for different operators. It is also possible to implement basic rules like it is for Store Value. For a card-based system, rules must be simple, like reduction if a means of transport from another operator has been used recently. In a centralized system, more complex and personalised rules may be implemented.

Closed Payment

Also referred to as closed-loop payment, the payment service is usually provided without any financial institution intermediary by the "operator" who is in a direct relationship with cardholders on the one hand and with merchants in the other. Well known Closed-loop networks include the likes of American Express who issue cards directly to consumers and serve merchants directly as well. Closed-loop networks also include retail brand-issued cards that can only be used in specific retail stores. When it comes to ticketing implementations, in many cases, merchants will be the transport service provider(s).

Capping

Capping is a rule to limit the amount that can be paid for a transport service over a given amount of time. It can be limited to an hour, a day, a week or more. Until such time as they reach the capping limit, passengers are charged based on the number of validations. Once the capping limit is reached, passengers are no longer charged until the end of the capping period. . Some simple ticketing systems are implemented according to this rule. Capping may be extended to more complex rules, including multiple operators.

1.4 Acronyms

Term	Description
ABT	**A**ccount **B**ased **T**icketing
B-O	**B**ack-**O**ffice
EMV	**E**uropay **M**asterCard **V**isa – Globally used for contactless bankcard, debit or credit and not limited to these 3 bank card schemes
NFC	**N**ear **F**ield **C**ommunication
P+R	**P**ark and **R**ide
PCI DSS	**P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandards
PO	**P**ortable **O**bject, i.e. a device used to carry transport rights (cards, phones etc.)
POC	**P**roof **O**f **C**oncept
PTO(s)	**P**ublic **T**ransport **O**perator(s)

2 VISION

2.1 Why ABT

Card-based systems in public transport use smart cards, or NFC enabled mobile phones, to store travel value, travel products (for example a monthly pass), discount rights (for example for students or the elderly), and tickets. Tickets can be pre-paid or Pay-As-You-Go (check-in check-out, or check-in only). Tickets are stored so they can be inspected.

In card based systems the fare calculation and applicative software are located in the different field equipment (validators, sale machines, inspection readers, …), i.e. the front office of the ticketing system.

Account Based Ticketing relies on two different principles:

- Firstly, the transport rights and contracts are stored in an account in a central server and not in the card or portable object
- Secondly, the fare calculation software and logic is located in the back office system and not in the front office equipment (validators, sale machines, inspection readers, …).

Consequently, portable object or card only remaining function is identification of the account, and terminals have no more ticketing applicative functions.

In other words, ABT offers the opportunity for transport operators to move the fare calculation software and logic away from the card reader to the back office (or 'cloud') where the account of the traveller also resides. The back office can then aggregate the transactions, apply algorithms to calculate the appropriate fare and deduct this from a recognized and trusted account. This could be a bank account, a credit card account, a pre-loaded account, or any kind of account that the transport scheme may trust. As the account is accessible online, any online changes to this account are immediately in effect, removing the need for a physical sales and distribution infrastructure.

ABT has been made possible following the huge increase in the throughput, reliability and speed of data communications; processing power in card technology; and the rise of the account is the online representation of a customer. Nevertheless, full online validation is not yet possible. For this reason, ABT often stays partially card based, for example for a local authentication of the card, without link to a server.

ABT only may be considered, for today, of a limited interest when 80 % of the journeys are done by persons with passes. This is applicable to public transport in most part of the world. For the other part, there is a substantial proportion of people without pass, but using frequently the same ticket for the same line. For this kind of travellers, ABT will not bring significant additional benefits. For the Public Transport Operators, ABT will not reduce the cost of sales for those passes and tickets. Today, the "closed loop" system is still an answer to the current needs of this kind of travellers at a lower cost for operators, but the economic model depends on the number of fare calculation software evolutions that are realized; if there are many, ABT can be an adequate answer to avoid costs of evolution on each equipment of the front-office. And also for

these passes, answering to the needs of new mobility players, such as bike rent, etc. may be facilitated by a centralized, account based approach.

The post-billing model (where the fare processing is moved away from devices onto host systems) allows an easier implementation of more complex rules, certainly in terms of interoperability.

With the system centric model, a variety of different payment models can be more easily introduced including:

- Direct billing to a cardholder's bank account via a pre-paid or regular billing model (like mobile phone billing);
- Linked accounts where families may have a single account for all family members paid for through a single payment means;
- Extending the linked account model to institutions, such as a company that may provide travel cards to employees as part of their salary package, and the institution is billed monthly by the transit operator.

One of the benefits of an account-based system for transit operators or authorities is the ability to create a variety of attractive products and partnership opportunities. Account-based ticketing and payments schemes can link a variety of appropriately secured "travel rights" or tokens to a single account. This can enable the introduction of innovative new models of linked transport modes such as park-n-ride, where the car license plate might be linked to an account and recognized through an ANPR (Automatic Number Plate Recognition) system, thus allowing for integrated parking and travel discounts.

2.2 Services to offer

The goal of an ABT system is not to replace existing passes, but to offer new services for occasional users or to offer complementary services to people with passes.

In fact, many tariff policies or services, that are presented as benefits from the ABT concept, could be offered to customers in a card centric approach, and yet it is very unusual today. The main reason is the complexity to develop such services with a card centric system; it would imply cards with a lot of memory and intelligence, and more, it will require developing complex software in the front-office, or worst, in several front-offices provided by different manufacturers; each evolution would require a full project, involving a large number of actors.

Consequently, the benefits of the ABT scheme for the customer are indirect: he will access to some tariff policies or some services only with an account, because the operator will offer these tariff policies or services only in such a way.

Pricing is not in the scope of this study, but pricing is a main driver for passengers to adopt ABT. If we offer with the ABT solution a monthly capping equal to the price of a monthly pass, many users may migrate from monthly passes to this tariff product. Yet, capping exists today with card centric systems, like TfL who

introduced it on a day basis with Oyster more than 10 years ago, but a capping based on an account management is definitively more flexible and cost efficient.

PTOs may still offer card based monthly and yearly passes and passengers are free to choose what is most convenient to them: card based or ABT.

ABT is particularly relevant for occasional users and new services. The main goal is to have an offer that is easy to understand and easy to use. Normally, people want to know how much they will pay before buying. Pricing rules must be clear and simple. The proposed services must also have an added value. Those services include:

- Carnets of ticket with daily capping and monthly capping, but as explained where capping must be/could be higher than daily and monthly passes price to preserve card-based passes. This is a choice in the pricing strategy.
- "Pay-as-you-Go" with check-in / check-out. This is useful for operators where the fare depends on the distance or number of zones.
- Interoperable product based on mono-operable ones; not combined, interoperable. For example: for 'P+R' the client pays for parking and transport with a combined product which grants him a discount when used within a certain period. Same approaches may be implemented for train + local transport or bus + bike.

The "Account" approach includes:

- Unique account for all services. If the user has an account, it can be used for all services, first of all, for public transport, but also parking or car sharing, cars, scooter or bikes.
- Prepaid and postpaid accounts.

  For prepaid, an amount is loaded to the account and an identifier is associated to the account. For tourists, it should be possible to have something like a smart ticket with a prepaid amount. Prepaid accounts can only give access to a limited set of services. The problem is that the amount will not cover for example the deposit for a bike. On the other hand, it is important to have a solution for the operator to avoid losing money when the lower limit is reached. Prepaid accounts are often card based, even if complementary rules are implemented on the back-end.

  For postpaid, the account can be linked to a credit card or to a bank account with an automatic debit. If in the future, a "global mobility budget" is developed to replace company cars, the account can be linked to such a budget.
- Anonymous accounts: This is usually only for prepaid accounts. You can link it to a card or a smart ticket.
- Third party payment, there are different approaches possible:

  P+R approach: the parking receives 1, the transport company receives 1. The user pays only 1,5 and the rest 05 is paid by the Public authority.

  Bill split approach: A "global mobility budget" or the employer can pay up to a defined amount per month. The rest is paid by automatic debit.

- Non-anonymous accounts can be associated with special concessionary profiles like 65+, student or family. In this case, the fare can be adapted to the profile.
- Bills can be sent, allowing to reclaim VAT or to use it as justification in tax declaration.

Remark: For managing prepaid accounts with a server-based approach, ideally validators must be online. This is probably not the best approach since card-based system pre-exists and validation time must remain very short. For this approach, a "card based" Store Value contract is the easiest, perhaps with back-end rules to adapt the amount. With the P+R example. If there are 50 on the card, 10 is deduced for the transport and 5 for the parking. During clearing, 5 will be adjusted by the public authority. Anyway, a back end must do the compensation between '*who has received and how much*', '*who has to be paid and how much*' and perhaps, '*where to go for third payer's compensation.*

2.3 Card-centric vs. System-centric

All the ABT possibilities and benefits are the consequences:

- whether from the storage of the transport rights and contracts in a central customer account, which gives a larger flexibility in terms of services to offer,
- whether from the move of the fare calculation and ticketing applicative software from the front office equipment to the back office, which greatly facilitates the development of new services and tariff products.

A system centric approach means a significant decrease in costs for the same level of services, or in other words, services which are not offered to customers today in card centric systems because of their costs, will become affordable in a system centric approach thanks to a better business case.

That explains the success of ABT for small new ticketing schemes which cannot afford to implement a card centric ticketing, out of proportion for the PTO in regard of the expected results and benefits.

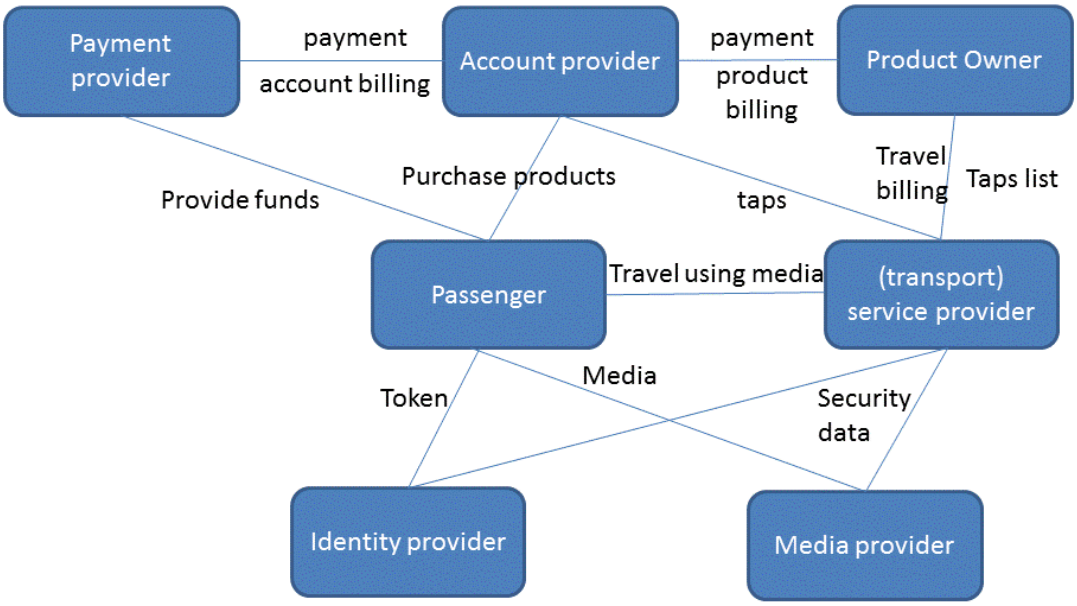
For the more important networks, particularly if they yet benefit from an existing card centric system, Account Based Ticketing is a strong opportunity to improve the tariff possibilities, with a dedicated target on occasional users of public transport, and to enrich the range of services to customers, in a multimodal and multiservice approach.

That means that, probably for many years, card centric and ABT schemes will go together for the benefice of both operators and users.

3 WHAT ABT IS ABOUT

3.1 The value chain (or rather maze) of ABT

The diagram below (from ISO/TR 20526) describes the relationship between the various stakeholders of an ABT scheme.



Account-holder relationship

An account can be linked to a person or a group of people. Depending on the case, a given person may be linked to one account, several accounts, or no account at all. The account can be anonymous in the sense that the operator of the account might not know the identity of the holder.

An account is a provider of rights. The lifetime of accounts can vary considerably. It can range from decades (in the case of bank accounts) down to days or even shorter (in the case of event-related and "disposable" prepaid accounts).

ABT and account-funding

Payment is closely linked to account-based architectures as accounts are closely related to transport rights. Accounts may be linked to a source of funds in the form of a traditional bank account. The link to the account may be embodied by the medium itself (e.g. bank card or bank chip or bank applet in Smartphone) or not. The notion of account also implies that the relevant information is gathered in a safe place which

can be seen as a virtual vault. Using a financial allegory, an ABT account would be seen as a bank account where the means to access the account may be varied and orthogonal (i.e. independent): channels and media. What really matters is the ability to safely access resources using appropriate media and channels.

Payment provider

The payment provider connects the scheme to the source of funds. It can take various forms. It can be a conventional bank. It can also be an independent or specific scheme. The common denominator of all payment providers is that they act as registered deposit taker (although they might not always be subject to banking regulations, this will be country-dependent). A given product will be associated with one or several payment providers. The customer chooses (much like in the case of online purchasing) a payment provider among the list available for a given scheme. The account provider makes payment requests to the given payment provider based on travel consumed by the passenger. The funds are then passed to the Product owner, subject to commission. An example of payment provider might be a scheme such as Paypal but some services providers operates themselves their own payment provider (ex: SNCF the National train operator in France)

Account provider

The account provider is the stakeholder that has a commercial relationship with customers. It sells products on behalf of the product owner. As in the case of media centric ticketing the products sold include tickets, season tickets, books of tickets and usage-based products.

Depending on the scheme and on the creditworthiness of the customers as assessed by the account provider, actual payment can occur at various stages or in a credit mode when travel has occurred.

Also, as in the case of media-centric ticketing, products can be either personalized or anonymous.

As the account provider charges customers for the transport usage, it must know what products the account holds in order to use the best possible combination. This can be an issue in the case where a user has several accounts. In the rest of the document we will assume that for the use of one customer only one account is used.

Account providers will ensure that customers can create and manage their accounts, verify the authenticity of the presented identities and entitlements and verify the authenticity and integrity of the transactions between customers and service operators.

In the case of usage-based products, account providers will register validation taps from the Service Operators reconstruct and price the journeys, provide the customer with an overview of all services they have consumed together with associated validation taps, and with the product owners manage a white list and a black list for all the tokens.

The account provider will inform Product Owners of the usage of their products and through product owners reimburse service operators the journeys travelled. In many cases, the account provider could be the transport operator, the transport authority or the ticketing operator.

Identity provider

The identity provider creates and provides a secure token associated with a passenger. 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 could be supplied later for storage on the media. It can also be supplied to be used anonymously, for example where the Product Owner issues tokens for anonymous use on the network of related Service Operators.

The identity provider is responsible for the security method employed for tokenization and 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 identity provider security scheme as only the service operator has equipment that is used to read customers' token. The Identity provider can be the transport operator or the transit authority if it provides its own token to the customer, but it could also be a bank, in the specific case of open Payment, or any service provider providing a secure token.

Product owner

The product owner specifies products based on travel services provided by service providers. The definition of the 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 (retailer) to sell their products to customers.

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 refunded.

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. Usually, the product owner is the transit authority or the transport operator.

(Transport) service provider

The service operator is responsible for providing the transport service to the passenger.

The service operator contracts with product owners the definition and sale of transport products. These contracts define travel services to be provided, the prices and conditions of carriage and the tokens and media 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 (validation) access control and (inspection) ticket control processes depending upon the calculation rules defined by the product owner. The service operator sends the validation taps to the product owner although in some cases related to usage-based travel the tap has to be forwarded to the account provider which is the only party able to correctly determine the best product for the passenger to use. Rules are needed in account-based ticketing scheme to accommodate late and missing taps.

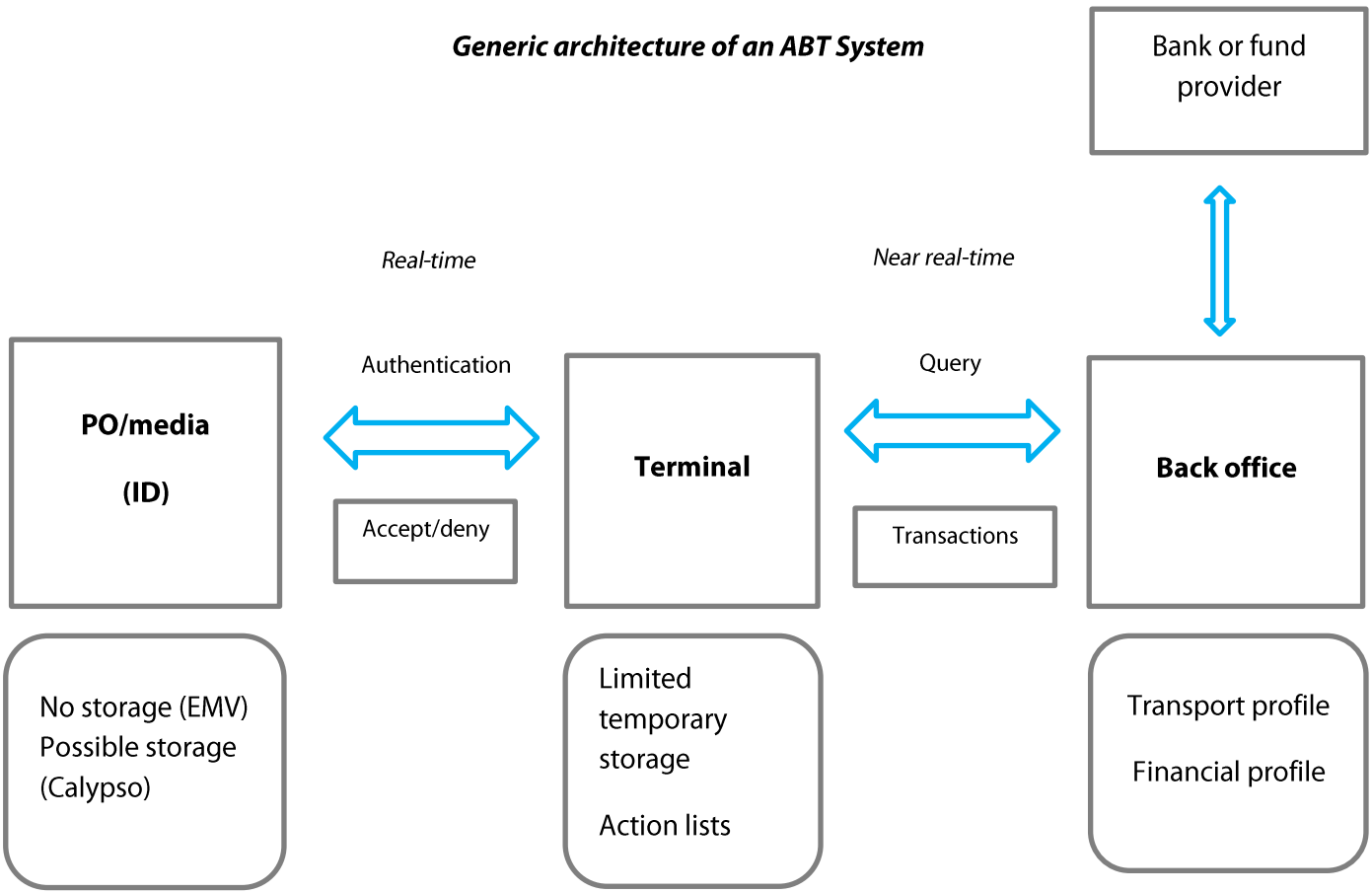
The passenger travels using suitable token as defined by the product owner. Taps on reader equipment or other checks of the token are sent to the product owner or account provider selects the best product for the travel undertaken and if necessary, calculate the price each tab contains information of the total service and the reader equipment. Can also contain additional other specific information such as time and location of the tap.

Media provider

Media used in ABT schemes exist in a variety of shapes and formats as the primary goal is to provide a secure identifier linked to an account. The media provider manages all the pre-issuance production processes resulting in the provision of either a medium personalized for a passenger or an anonymous medium. The media provider is also responsible for dealing with the medium at the end of its life-cycle including decommissioning. The media provider is responsible for the security method featuring in the medium and by making sure that the system can handle the security provided they also implement the appropriate security algorithms. The media provider is responsible for providing the required security data used in the system. The media provider can be the transport operator or the transit authority if it provides its own media to the customer but it could also be a bank, in the specific case of open Payment, or a phone manufacturer (or smart phone OS maker) in the case where the secure token is stored in a smartphone.

3.2 Classification of ABT Mechanisms

Generic architecture of an ABT System



In the ABT scenario, the credit/value/entitlement is not on the card but in a back-office account (be it a bank account, a dedicated travel account or otherwise). If the validator is online, the appropriate credit verification and debit can take place instantly. If the system allows for records to be written on the card/PO, information regarding available credit can be recorded and used by validators. Otherwise granting travel rights based just on the ID of a card/PO incurs risks that the travel rights might not be paid for eventually.

Here are several ways that risks can be addressed. This gives rise to a classification into three categories:

3.2.1 Full on line access

If the account can be accessed during an online validation, a secure transaction can take place and credit can be used or a deposit taken.

3.2.2 Differed rights control

If the account cannot be accessed during an online validation, the validator can check that:

a) the PO is genuine and

b) that it is not hot listed (blacklisted).

This assumes that hotlists include all permissible POs that are not creditworthy at a given time, i.e. for which at the end of a given period may not be used for paying transport rights. Hotlists are updated regularly on all validators. This approach is that of TFL (London). The risk in this case is that a card will not have been on the hotlist at the time of validation but will have gone out of credit before the payment transaction goes through, in which case it will be hot listed but the passenger will have travelled regardless. This case is very rare in the case of credit/debit cards as the process of getting a card is time-consuming and, depending on the country where it is issued, potentially expensive. The value of bank cards is such that the risk described above is very limited and therefore generally considered acceptable.

3.2.3 Pre-authorized rights

If the account cannot be accessed during an online validation, an alternative can be envisaged in the case where data can be securely stored and read on the card/PO. The idea here is to record information on the card to help validators decide whether or not to accept a given card/PO. Instead of relying on hot lists, the card/PO registers pre-authorized rights. Every time a validation is performed, the validator will check the locally stored pre-authorized right. If there are no more rights the validator will inform the user, and if there are remaining rights, decrement them and send the information to the back-office as in the case of all ABT validations. The locally stored pre-authorized rights are updated by the system when relevant, e.g. when a chip and PIN transaction takes place.

3.2.4 Pros and cons of the three solutions

	Full online access	Differed rights	Pre-authorised rights
Authentication	Online or offline	Offline only	Offline only
Risks & usage restrictions	Limited risk if connectivity is operational. The validation time depends on the quality of the connection	"First travel" risk Inspection challenge Requires high frequency hotlist updates to limit the risk	Limited if pre-authorized rights are present. Otherwise could require an online connection to update differed rights
Inspection without transaction log	Online. Issue if validations uploads are postponed	Is an issue unless one recovers validation taps directly from validators	

In systems that allow recording logs, recording the last validation taps (events) allows for off-line inspection, which can be very useful whenever validations uploads are delayed or absent.

3.2.5 Downgraded Modes

As described earlier, ABT relies on the assumption of high availability networks. Here, for each category of ABT, we describe what downgrading means and what solution can apply.

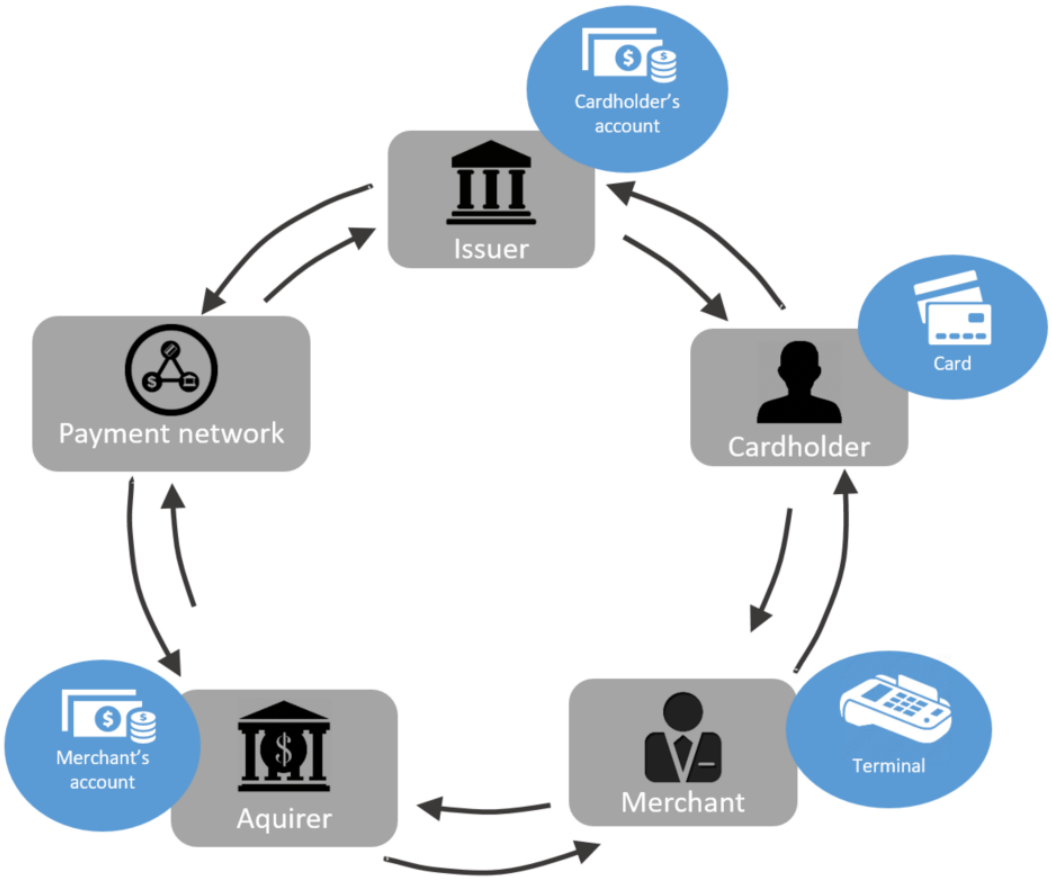
Mode	Downgrading	Downgraded solution
Full online	Loss of network connectivity	Fall back to differed-rights if off-line authentication is possible
Pre-authorized rights	Preauthorised rights limit reached	Trigger online connection to update rights during validation
Differed rights	Long period of connectivity loss	Accept increased risk…

4 THE SPECIFIC CASE OF OPEN PAYMENT

4.1 Definition

Open Payment in ticketing is a specific case of ABT where the media that are used are contactless bank cards, which can also be used for paying non-transport-related goods and services. There are several ways to implement such services.

The major attractions of the use of contactless bank cards lie in the fact that they are inherently interoperable (banks have decades' experience in ensuring interoperability of cards with readers and back-offices), they are widely deployed (although not all travellers hold bank cards: children, the unbanked), most people travel with them (no need to remind people to take a bank card with them) and issuing and aftersales service are performed not by transport stakeholders but banks.



One other major benefit of bank card centric systems is that they do not require opening up or toping up dedicated accounts as they are linked to existing bank accounts.

EMV, like other credit card process involves different actors:

- **Acquirer**: An Acquirer is an organization authorized by the payment schemes to enable merchants to process debit and (or) credit transactions. The acquirer establishes a contractual relationship with the merchant and assigns the relevant fees/discount rates for the merchant and ensures the merchant complies with all regulations stipulated by the card schemes.
- **Issuer**: The financial institution who issues the credit or debit card to the customer or consumer.
- **Cardholder**: The client, the person using the transport
- **Merchant**: For transportation, this role is assumed by the PTOs, PTAs or retailers

4.2 EMV Contactless certification

One major benefit of bank cards centric schemes is that they rely on cards for which the certification is very thorough and a virtual guarantee of interoperability between cards and terminals.

EMV products both on the PO and the terminal side are subject to certification, which includes pairwise testing with dual-type equipment: Cards are tested against reference terminals and terminals are tested against reference cards. Evolutions occur every so often and EMV Co ensure product compatibility. Product certification has been central to banks business, which translates in the fact that interoperability is very successful.

For EMV, the validator (and the whole chain up to the Acquirer) must be PCI DSS Certified. Payment Card Industry Data Security Standards (PCI DSS) compliance mandates that all organizations that accept, acquire, transmit, process, or store cardholder data must take appropriate steps to continuously safeguard all sensitive customer information.

4.3 Buying transport rights from POS terminals

A much-publicised experiment is that conducted in Grenoble where a few bus lines have been equipped with EMV contactless POS terminals. In effect, it is closer to a pure retail application than a ticketing application. There is no notion of optimised fare generally associated with Open Payment. In the case of the Grenoble experiment, every validation translates into the immediate payment of a flat fare, which can be convenient in some cases but does not cover the range of services expected by most authorities.

In these implementations (South Africa, Grenoble), validators incorporate EMV contactless POS terminals. Validations are fixed fee EMV contactless transactions producing the same result as if a merchant sold a service for the same amount. It makes use of the EMV Contactless mechanism used for small value purchases. The underlying principle is that EMV allows to perform a number of off-line contactless transactions. The total value, the number of transactions and the maximum time a card can be used in that mode before it needs to go through a chip and PIN transaction depends on individual banks. When a chip and PIN transaction occurs, counters are reset as this transaction testifies that the card is in the hand of its rightful owner.

Benefit

- Using an existing and proven mechanism

Shortcomings

- Suitable for flat fare only
- Every tap generates a purchase
- Ticket inspection is based on the ticket printed by the POS
- System not integrated in the ticketing system
- Potential issue when insufficient credit is available

4.4 Using EMV contactless bank cards as secure ID media

Another approach consists in checking that a card is genuine and has not been black listed when it is used for validating. This is the TFL approach.

In standard EMV contactless transactions the card has an authorization for a small amount until the next chip and PIN transaction, typically maximum 20 Euros and when it is used, the counter is decreased from the amount paid. The transaction can be done offline. When the amount is reached, an online connection and/or PIN transaction is necessary to authorize the payment and reset the counter. This is seldom implemented like that in transport.

Validators check that the card is genuine, acceptable and not hot listed. This is performed in real time and does not require an online transaction. Then a £0 transaction is triggered for every tap. Validators hotlists are regularly updated.

General contactless payment rules	Agreed new rules for transport
Price is known before the card is presented	Each tap of 0€, then the operator back-office calculates the price typically at the end of the day.
Use of card counters to manage risk & occasional revert to Chip & PIN	Operator bears the risk to provide equivalent protection within the 500ms time limit: - Offline data authentication of card - Deny Lists in terminals - Online authorizations from the back-office
Terminal RFID field is activated manually by store staff	Terminal field is always active to maximize throughput.

An authorisation for an amount greater than the maximum trip is requested from the back-office to the bank. If the requested is accepted, this reserves the amount and therefore guarantees payment. If the request is denied, the information is then sent to validators to update the hotlist. This has for consequence that the first usage is always allowed. The issuing bank will cover the cost of the very first trip, even when the account was blocked.

Benefits

- Suitable for a wide range of cards
- Suitable for varied tariffs

Shortcomings and requirements

- Requires specific back-office processing
- Financial Risks (including "first trip risk")
- Requires validators to be online or near online
- Ticket inspection can be a challenge (see section 6.2)

5 ABT AROUND THE WORLD

This chapter merely gives an overview of some projects. It is far from being comprehensive and does not attempt to be so.

UK

- The TFL (London) system is most often frequently quoted system. It is based on the use of EMV contactless cards. It provides best pricing by integrating all the taps performed by users and applying the most relevant tariff, including capping. It is available on all TFM transport modes (bus, tram, train, DLR, Tube etc.). The back-office system was designed and built in house by TFL whilst the upgrade of terminals was funded by the Department for Transport.

USA

- The USA is the country where it all started: CT DOT in Connecticut, NFTA in Buffalo, Portland, Oregon, MTA New York City Transit, Port Authority Trans Hudson and New Jersey Transit

Europe

- The BKK network in Budapest is an early implementation of ABT. It makes use of various types of POs, including but not restricted to bank cards.
- Turku is the first network in Finland to have implemented ABT.

France

In France, Open Payment generates a keen interest from Transport Authorities, in particular for dealing with occasional users.

- The TAN (urban transport network in Nantes) proposes an ABT service based on smart card (Calypso and Mifare) with a post payment system.
- Bordeaux will have an open Payment system will be available in the summer of 2017 which will include daily capping.
- Greater Nancy, Nantes Rennes all envisage implementing open payment schemes whilst other French authorities have expressed an interest (Angers, Dijon, Marseille, Toulouse…).
- Grenoble has implemented a system where validators behave like POS terminals (see 4.3)

6 BENEFITS AND SHORTCOMINGS OF ABT

6.1 Benefits

Simplified sales infrastructure

As tickets do not need to be physically reloaded, sales can take place anywhere, including online, thus alleviating the cost of distributing and loading products on cards/POs.

Standard off the shelf products

As the terminals are limited to authenticating cards/PO, checking that they are either white-listed or not black-listed and communicating with the back-office, they remain basic in design (bar the potential security constraints, such as specific (e.g. EMV) certification) and therefore can be considered as off-the-shelf products. Scheme owners can easily change suppliers for that reason. Also, as the processing they perform is independent of the back-end processing, they need not evolve much over time. ABT is therefore futureproof and cost-effective.

Fare flexibility

ABT allow to perform smart and personalised tariff computation. Given that processing occurs in a back office, the actual tariff does not need to be determined at the time passengers enter or exit the network. It can be determined through possible aggregation on a daily basis or even a weekly basis based on multiple criteria including times and places of validations (entries and exits), time of day, special events and circumstances (disruption etc.).

New tariffs need only be implemented in back-office systems. As back-offices deal with all validations, the system can apply smart tariffs such as capping or event-specific tariffs (e.g. provide discounts if the quality of transport service was poor) etc. The sky is the limit.

Manageability and scalability

ABT systems are inherently modular and scalable. Synchronising, administering, and maintaining the data in the whole system is rendered a lot easier compared with card-centric systems as the data essentially flows directly from cards/POs to back-offices whilst terminals tend to be neutral in the process.

It is also possible to combine card centric and ABT systems and seamlessly migrate from the former to the latter. In the case of existing Calypso networks, this means that there is no need to change the current equipment to migrate to ABT. Networks can retain their Calypso infrastructure and migrate part or all of their POs to ABT. Calypso networks can accommodate the simultaneous use of both PO-centric and ABT. When a card-centric and a ABT system coexist, the full financial benefits of reduced costs are only achieved when the migration to ABT is completed. Until such time, the software maintenance costs actually add up. Networks however usually need to be upgraded to provide near real-time connectivity.

Limited requirements regarding cards/POs

In all strictly ABT systems, no data is written on cards/POs. Essentially, readers read the ID of the card/PO and ensure that it is genuine. This means that any device that is able of securely providing this information can be used in ABT systems. Naturally, in cases where the implementation of ABT is done according to EMV contactless specifications, cards/POs need to be EMV-certified.

Comfort for users

As no value is stored on the card/PO, losing a card/PO does not result in the loss of the value on the account. Relying on EMV-contactless specifications means that travellers holding EMV contactless cards can validate using their own card and do not require a card issued by transport authorities or operators.

6.2 Shortcomings

ABT systems rely heavily on the availability, the quality, the efficiency, and the low latency of networks. Shortcomings relate to the following:

Network availability shortcoming

Traditional ABT systems rely heavily on networks as transactions are processed in a back-office server, which is not available when the network is down. As in "pure" ABT schemes there are no means of recording data on media, fall-back strategies are limited:

ABT terminals can buffer the transaction request and send the request to the back-office when the network connection is resumed. In that case, the terminal takes the risk of emulating a successful transaction for media that are linked to accounts that cannot be charged for lack of funds or for any other reason. In that case, bona fide customers will travel for free and any query made to the system by some inspection device (whether it be by performing a query to the back office or to the validator) will show either no transaction or the fact that the customer has indeed validated. In such circumstance, it is not possible to fine the traveller.

The alternative solution is to refuse all transaction which means that customers know that the transaction has failed but have not means to validate, which is not helpful either.

Existing solutions can rely on the use-coloured lists in the following manner. Terminals synchronise acceptance (white) and deny (black) lists as frequently as possible. The subsequent strategy is to check any portable object ID against both lists. If the portable object's ID is on the blacklist, then the validation fails although the account might have been credited since the last synchronisation. If the portable object is on the white list, then the validator might accept the validation although the account might no longer be creditworthy. If the portable object is not on any list, then the validator will probably not validate the portable object. This strategy is prone to errors, generates significant customer complaints and could potentially result in significant revenue losses. Furthermore, synchronising those lists in validators requires managing large memories, processing and using up potentially valuable bandwidth.

Concessionary profiles

As "pure" ABT POs only contain an ID, unless a network connection is available, there is no way for a terminal to ascertain whether the PO holder is entitled to concessionary fares. Existing systems often highlight the concessionary status of users to facilitate inspection.

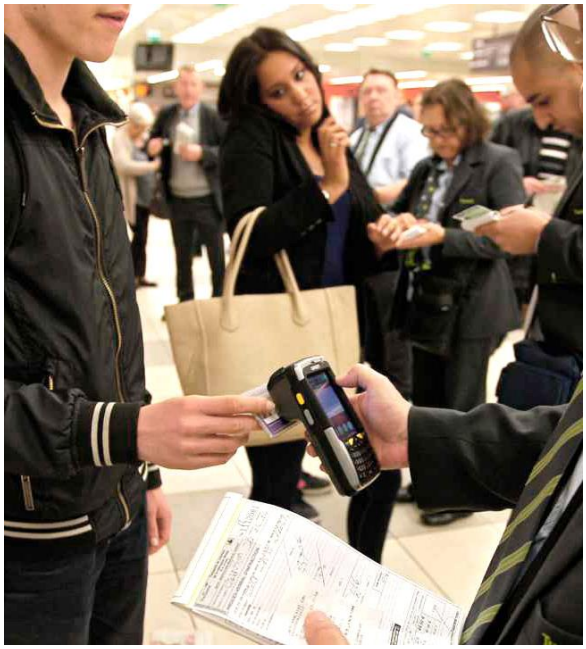
If a traveller uses a concessionary account and if there is no sign on the portable object whether graphical or electronical, then anyone could use such portable objects and not be detected as fare evaders during inspection unless the ticket inspection machine connects to the account database.

Ticket inspection

As the information relative to ABT transactions is registered in back-office (and optionally in validators in addition to being stored in back-office), inspecting POs also requires accessing the back office system. This can be challenging and time-consuming as inspection terminals suffer from the same network failures as validators. One alternative that is used consists in reading the log from validators. This can only be successful when the inspection is carried out where the traveller is near the validator when being inspected. In other words, it can only be relevant if the inspection is carried out on board a bus (resp. a tram) which is serious limitation.

In metro, train, and in some bus and tram networks, ticket inspection is performed away from the validator/gate which means that relying on accessing the data directly from the validator/gate used by the traveller for inspection purposes is simply not feasible.

The use of mobile networks can give rise to high latency which in turn translates into angry customers as inspecting a PO can take several seconds. In a different sector, new car parking systems often rely on the use of number plates. Car drivers enter their car number plate into a system when paying for parking, e.g. through a smartphone application. Parking inspection then relies on the use of 3G/4G connected devices, which takes several seconds for every car. In the case of car parking, the speed of inspection defined by the number of parked cars checked by time unit is not critical from the user (driver) point of view as he/she does not need to wait. However, in the case of ticket inspection in public transport, time and throughput are critical. To be acceptable by passengers, ticket inspection must be very efficient. Therefore, ticket inspection can be the Achilles' heel of ABT systems unless robust solutions can be found to ensure it can be carried out efficiently, regardless of the 3G-4G network.



Risk management

As ABT schemes need to access the back-office server not only to register the transaction but to prevent it when the PO is either not linked to an account, linked to an account that has tempered with or linked to an account that has insufficient credit or rights, the unavailability of the network at the time of the transaction means that if the fall-back mode of the validator is to let passengers through, then the system takes the associated risk.

Data centralization

In a system centric approach, data (transport rights, validation events, etc.) are no more stored in customer cards, but in a central server. It brings a significant advantage for on-line sales service. But it also implies concentration of all customer data in a single point, which may be considered as a weakness. First because, all data could be lost in a computer crash; of course, backups are available, but data recovery is always a sensitive issue, which quite never goes on as planned whatever the software engineers may say. In card centric approach, everything is local (data storage in the card, tariff software in the validator), and there is less probability of an extended crash. Secondly, because customers data concentration generates interest to the hackers, and therefore data privacy is an issue to be taken into account.

Shortcomings specific to Open Payment systems

Implementing an Open payment scheme implies using bank cards as POs and relying on banking infrastructure. This translates in the following consequences:

- Writing a secure application/token on an bank card is not allowed. Then the card only is not enough for inspection.
- Some people are averse to getting their bank cards out of their bag/purse etc. in congested places such as public transport network as they do not feel safe. This will differ from country to country.
- Some people do not have or use bank cards. This again will differ from country to country.
- Most underage children do not hold bank cards.
- The costs of using the banking infrastructure might in some cases turn out to be prohibitive. Public transport is reputedly a small-margin business and therefore more sensitive to margin erosion than most other businesses.
- Open payment forces the use of bank accounts. Non-bank card centric schemes provide more flexibility regarding means of payment.
- The brand of the transport authority/operator does not usually appear on bank cards: in order to keep control of customers, some authorities envisage using their own branded cards, and in some cases multiservice cards, whilst envisioning open payment essentially for occasional users.

Susceptibility to hacking

In ABT systems, accounts can potentially be more easily compromised as they are centralised. There is more incentive to hack a centralised system as doing can bring the whole system down as opposed to just a few accounts. This is made all the easier as ABT systems tend to do away with such filters as concentrators.

Certification

The purpose of certification is to ensure that a given service operates consistently according to specifications. In the case of ticketing, the purpose is to ensure that validations are successful and that data are consistent with specifications. The absence of certification can be an issue as it can lead to lack of interoperability between POs and terminals.

Interoperability

As in ABT systems POs are used merely for identification purposes, one same PO may be used by several networks and be linked to several accounts, e.g. one per network.

When a traveller uses his/her PO outside the network on which it is linked to an account, it will be treated as unknown and therefore its bearer will be denied transport access. With the notable exception of bankcard-centric schemes, such as London's, there is no standardised ABT mechanism to deal with interoperability.

PO security

ABT systems rely on POs being used solely for linking its bearer to an account. This can give rise to account hacking through cloning POs.

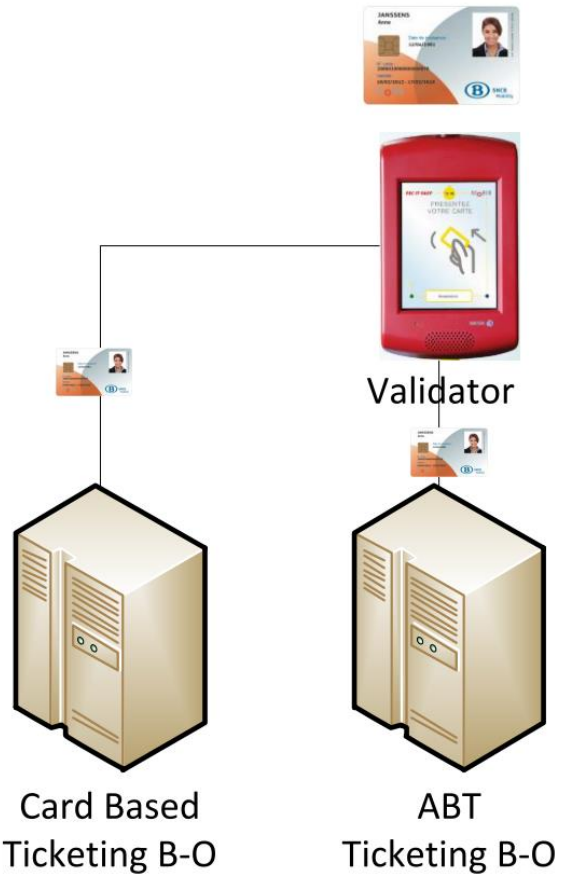
In some sectors, such as air transport or long-distance trains, cloning POs might not be an issue as the validation process can require actually checking the ID of the bearer. Inspecting POs can take several seconds but this amount of time is acceptable as the passenger throughput is very limited. In public transport on another hand the ID of bearers is rarely checked, and cloning can be a more significant issue. Cloning bar codes can be achieved easily by the man in the street. Cloning Mifare cards is no longer a challenge. Therefore, cloning can be a significant issue for public transport ABT schemes.

7 ARCHITECTURE

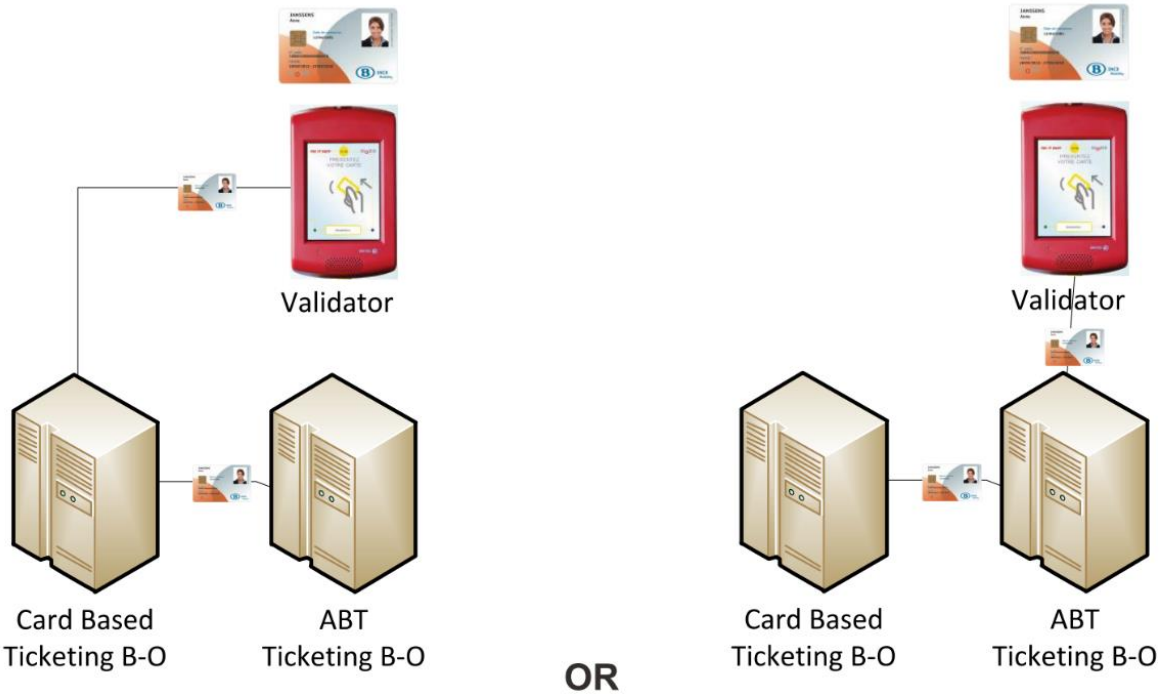
7.1 ABT without or with EMV

If ABT is not based on bank cards, there is no contractual need for a PCI certified path. In this case, a payment Back-office is not necessary. The same architecture can be used for ABT and Card Based. It can even be the same system if it is limited to one operator or to a shared system.

In the following architecture, validations are split by the validator:



But it is also possible that all the validations go first to the card based back-office and then, only ABT validations are transferred to the ABT back-office. Alternatively, it is possible that the ABT is before the card based B-O. The major benefit of such a solution is that no modification is needed at validator level.



The way to implement-it to have a minimal change on the back-end is the following:

- Two contracts must be created:
  One contract for anonymous prepaid value contract. This contract can be renewed like normal contracts. This contract has the remaining value as counter.
  One contracts for post-paid ABT approach. This contract has a validity period and for the rest is like a LP.
- Adaptation must be done on the back end to send all the validations to the calculation engine.
- Adaptation must be done also to accept return of calculation for 3 aspects:
  Adaptation to counters on card anonymous value contracts to pay back amounts due to capping or interoperability rules.
  Amount to be invoiced for postpaid contracts
  Amount to be paid to other actors for post-paid contracts

For post-paid accounts, the ABT contract will be similar to a pass with a validity period corresponding to the payment authorization period. It can be renewed with a new authorization. The contract can also be black listed if the account is disabled before the end of validity period.

"Classical",i.e. card-based, contracts have priority on the ABT one. ABT is only used when no other contract present on the card can be used.

For prepaid-anonymous contracts, it must be checked that the user does not exceed the prepaid amount. Because it is impossible to have all the validators permanently online, there must be an amount counter on the card. Interoperability rules like P+R for example, and rules like "pay less for a second trip" or capping rules can be managed from the card or by the backend and refilled the card via green list. In any case, the back end is mandatory for revenue distribution.

Prepaid cannot be used for all service. For bike sharing, for example, even if the rental cost can be covered, the price to be paid if the bike is lost cannot be covered.

7.2 EMV contactless architecture

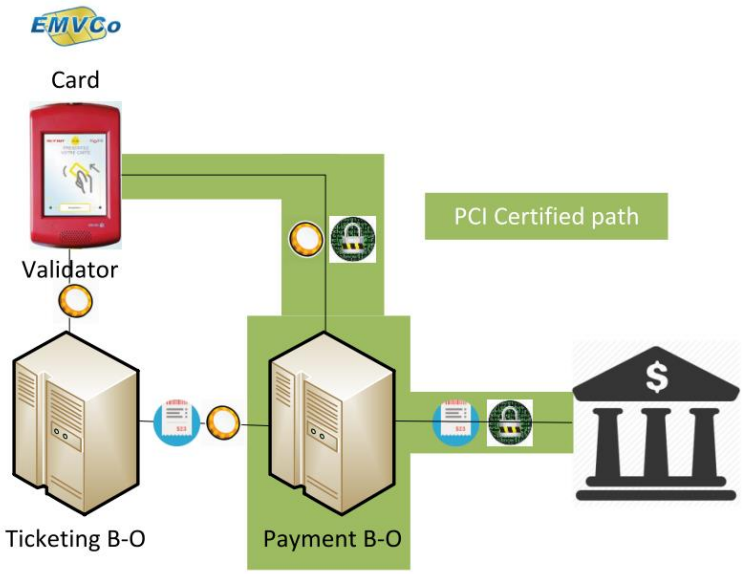
The classical EMV contactless architecture is the following

It is virtually impossible to have a full back end certified. A parallel path is at least necessary for payment.

The Payment B-O is limited to payment functionalities. There is no "card info" in the ticketing Back-office. ABT rules are processed in the ticketing B-O. If the two Back-Offices are not separate, the full system must be PCI certified and the certification must be carried out each time a rule is changed.

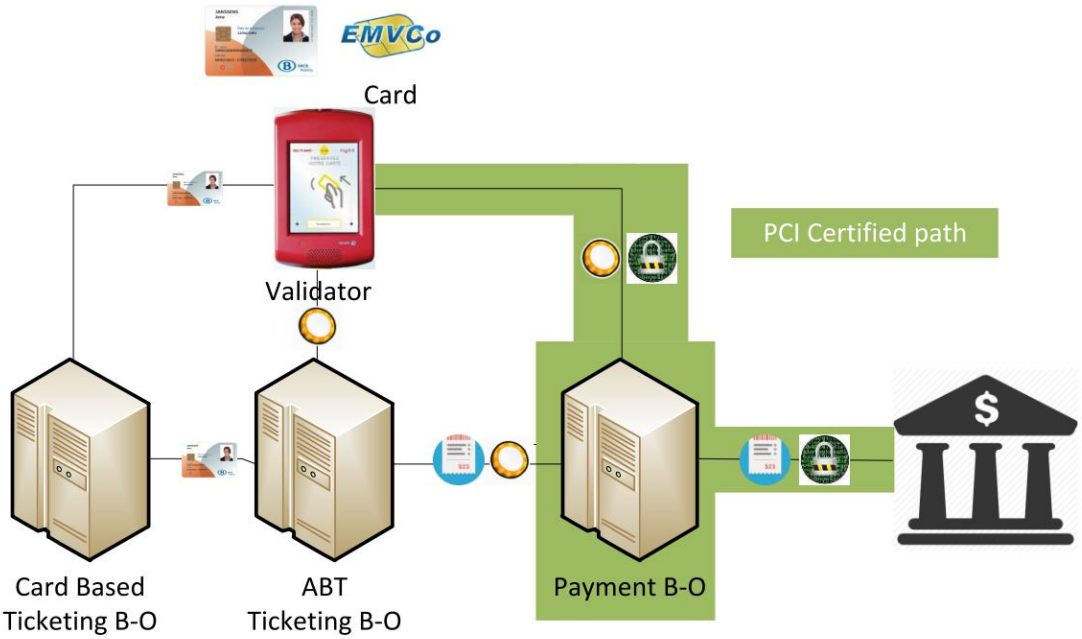
It is also possible, and it is often done, to have a completely separate EMV with dedicated rules.

It might not be a problem to have two validators in the same bus.



It is also possible to add ABT on this model. In this case the scheme will look like the following:

In any case, Payments linked to EMV, must go in a separate flow to avoid to re-certify the full chain each time a modification is applied. With a system like this, it is possible to apply the same ABT rules for users using EMV in place of pre-registration.



8 CALYPSO IN THE ABT ECOSYSTEM

ABT systems in the conventional sense of systems that rely on POs solely for identification purposes and linking those POs to accounts, have shortcomings that can cause major issues (slow inspection processes, revenue losses etc.).

As seen in 6.2, in many cases, Calypso can address these issues.

Calypso is well known for providing a secure ticketing environment.

The issues where Calypso can provide a solution are:

- Addressing Network availability shortcomings
- Dealing with Concessionary profiles
- Ticket inspection
- Interoperability between networks
- Being tied to banks and bank card schemes
- PO security
- PO/terminal interoperability

Here are ideas as to how Calypso can deal with the various issues:

Dealing with Concessionary profiles

→ Calypso opportunity to be developed: write in a standardised manner the flag that identifies the portable object as relating to a concessionary account. Other similar data might be stored such as profile or photograph.

Ticket inspection

→ Calypso opportunity to be developed: Register the transaction on the Calypso ABT PO so that inspection can be carried out efficiently without the need for network coverage.

Risk management

→ Calypso opportunity to be developed: Record transactions on the Calypso PO, in such a way that in the cases described in 5.1, the validator will signal to the traveller that the validation is unsuccessful. The risk in that case is if the traveler has in the meantime credited his/her account but that the credit operation is not reflected on the PO. In that case it could be useful to record a “differed right” readable locally by the validator in the PO when the account is credited, in order to avoid the customer being rejected if the White/Black lists are not updated fast enough.

PO certification

→ Calypso opportunity to be developed: Calypso certification
CNA and PayCert (a subsidiary of GIE CB) got together to certify the communication between card and readers. Products have already been certified.
STA (The Smart Card Alliance) has defined a certification process. The stakeholders include CNA, ITSO, VDV and AFIMB.
The GSMA and NFC Forum have reached an agreement by which GSMA defines a certification process for mobile handsets whilst the NFC Forum defines a certification process for terminals. The processes are defined in such a way that it ensures that GSMA-certified handsets interoperate with NFC Forum-certified terminals.

Interoperability

→ Calypso opportunity to be developed: Calypso can provide solutions to address this shortcoming based on the high security level of Calypso POs, the existence of a unique ID, and the use of Triangle 2 which can be adapted to the ABT context.

PO security

→ Calypso opportunity to be developed: Use of Calypso POs to prevent cloning. Also, by securely identifying a Calypso PO, we can establish that it holds a deposit and whether the deposit has been used or not.

In some cases, Calypso can provide a solution straight away. In other cases, Calypso could address them pending evolutions to the Calypso specifications.

Other aspects that could be covered include:

- Standardising differed rights mechanisms
- Defining a solution for regular users

9 CONCLUSION

Account-based ticketing is on many transport authorities' agenda.

Open Payment, especially EMV contactless based, is one specific implementation of ABT that has been successfully implemented. Key benefits include the fact that card issuing and after sales service are covered by third parties (banks), enrolment is automatic for bank customers and interoperability is mastered successfully. The drawbacks of Open Payment and ABT schemes more generally are the fact that network failures and disruptions are problematic, that ticket inspection causes feasibility and legal issues, that the management of concessionary card holders is complex, that centralization of all customer data represent a weak point and a privacy issue, and finally that it removes some of the independence of transport authorities and operators

Our work must now go into two directions:

- The first one is to provide guidelines for those who intend to migrate from an existing card centric solution based on Calypso, to a system centric solution.
- The second one is to investigate how to solve the identified shortcomings and propose improvements that could be brought to the standard ABT approach by using Calypso features.

This requires going further in the analysis by clearly evaluating the topics linked to the card centric approach (storage of data in the card), to the front-office centric approach (ticketing software in the validator) and to the back-office centric approach (storage of data and ticketing software in a central server).

Based on this analysis, the split of functions between the different components of a ticketing system could be optimized, and leading ticketing to a step forward, for the benefit of customers, authorities and operators.

ABOUT CNA

Calypso Networks Association is a non-for-profit association established in Brussels in 2003. The main objectives of CNA are to define and direct the reference specifications, to implement a certification policy, to guarantee the compatibility of all current and future product and to establish a Calypso label issued by an independent organization.

Founder members of the project: OTLIS-Lisbon, ACTV-Venice, STIB-Brussels, LKRKN-Constance and RATP & SNCF-Paris. Calypso is the contactless electronic ticketing standard designed by users for users.

www.calypsonet.org

Contact : contact@calypsonet.org
Cour d'Avril, Passage du Cheval Blanc 2 rue de la Roquette, 75011 Paris, France

ABOUT BMC

Created in 2010, BMC is A joint subsidiary of SNCB, STIB, TEC and De Lijn

Which carries out the conceptualization and development of a common ticketing system for passenger transport tickets in Belgium.

http://www.mobib.be

ABOUT RATP SMART SYSTEMS

RATP Smart Systems is a subsidiary of the RATP group specialized in the development of mobility assistance services. With 200 employees, it designs, integrates, operates and maintains systems for ticketing, multimodal information and operational support (presence in 115 networks). The company also operates the Paris and suburban ticketing system (12 million transactions per day), the largest multimodal network in the world with the presence of metros, buses, tramways and RER.

https://www.ratpsmartsystems.com/en/accueil-en/