Connected Mobility

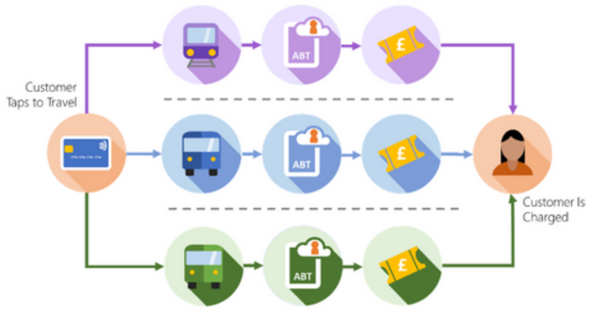
Enabling Interoperability between Contactless (cEMV) Pay As You Go (PAYG) Ticketing Systems

May 2023

TRANSPORT FOR THE NORTH

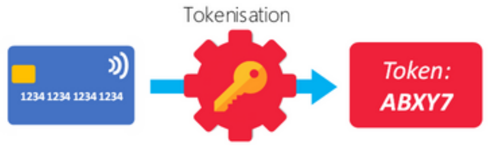
Executive Summary

As delivery of single Operator contactless PAYG capping continues, central government, statutory bodies, Local Authorities and Operators are increasingly keen to introduce multi-modal/operator PAYG with Capping to incentivise customers to use public transport services.

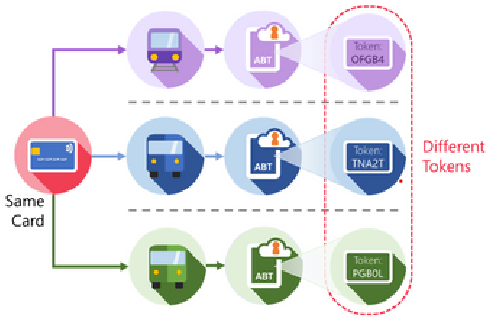


Current contactless PAYG propositions are delivered by different ticketing system suppliers, who have developed subtly different solutions to protecting the cardholder data that is generated when a customer taps their contactless payment card, and that is used to charge the customer.

A common solution to protecting cardholder data stored and processed by ticketing solutions is Tokenisation, which converts sensitive contactless payment card information into a non-sensitive equivalent, called a "Token", allowing it to be processed safely.



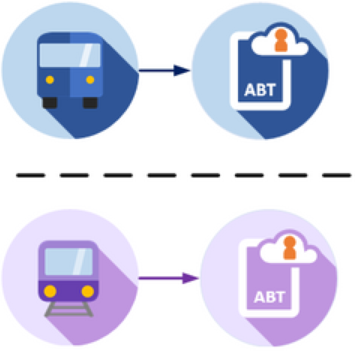
Currently, each ticketing system supplier creates its own Token for each contactless card they see used on their services. Each supplier's Token will differ from each other.



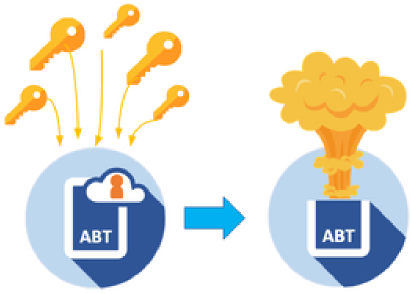
To enable multi-modal/operator PAYG using contactless payment cards, each existing ticketing solution would need to interface with each other or a common multi-modal back office and share the journeys and charges made by each individual card.

However, the payment industry standards designed to protect cardholder data discourage payment card details from being shared between systems. Each individual ticketing system Token is different, meaning that they cannot be used to identify the same card journeys and charges which are required in order to identify multi-modal/operator caps.

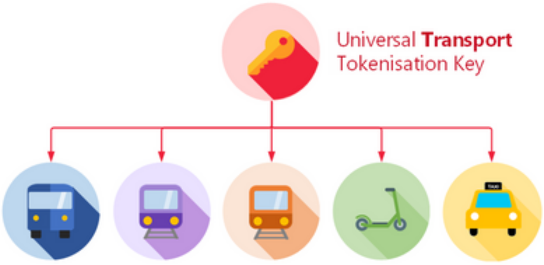
Whilst the concept of consistent tokens used for interoperability has been discussed in the transport industry for some years, there is a risk that, if a project considers this modally at first and defers multi-modal consideration to a later date, the eventual multi-modal solution will be much more challenging to deliver than if considered in advance.



Failure to consider how cardholder data can be protected when used across multi-modal and/or regional PAYG solutions risks the industry inadvertently finding themselves in the situation where the only option to deliver multi-modal capping requires complex integrations requiring the use of multiple different tokenisation mechanisms to enable the various systems to talk to each other.



The introduction of a Universal Transport Token, a consistent mechanism to protect cardholder data across any operator or mode, could provide a consistent Token for every customer payment card, thus significantly simplifying multi-modal integration cost and risk, plus simplifying many business processes (e.g., customer services)



Parties involved in the development of modal or regional contactless PAYG solutions would therefore benefit greatly in working together at the early stages of their projects to avoid requiring these overly complicated solutions for integration at a later date, that would duplicate effort and costs and be much more difficult to maintain.

It is acknowledged that introduction of the Universal Transport Token will require active engagement with all contactless PAYG projects currently being developed in the UK, and agreement from participating stakeholders to agree and adopt a single approach (via a single supplier, likely owned by a neutral party) to Tokenisation in transport – but the longer-term benefits to enabling multi-modal integration will justify this initial intervention even if full delivery is required later.

Introduction

Most Operators and Transport Agencies have rolled out contactless acceptance as a retail payment method to purchase tickets. Subsequently, focus has shifted to enabling customers to make Pay As You Go (PAYG) journeys with capping using their contactless card to validate as they travel.

Because Operators are delivering this capability on their own services, each operator can only cap and charge customers for travel on these single operator services

The downside for the customer is that if they make one journey on each of three different operators services, they will not achieve any Operator Cap, and they will be charged three separate charges. This means that using post-pay contactless PAYG can be more expensive than a customer purchasing a multi-operator ticket in advance, or using multi-operator ticketing schemes where they exist.

As contactless PAYG becomes widespread, the customer expectation and the desire of central and local government is to enable customers to benefit from post-pay multi-operator and multi-modal capping, delivering a "London-like" experience in more regions of the UK.

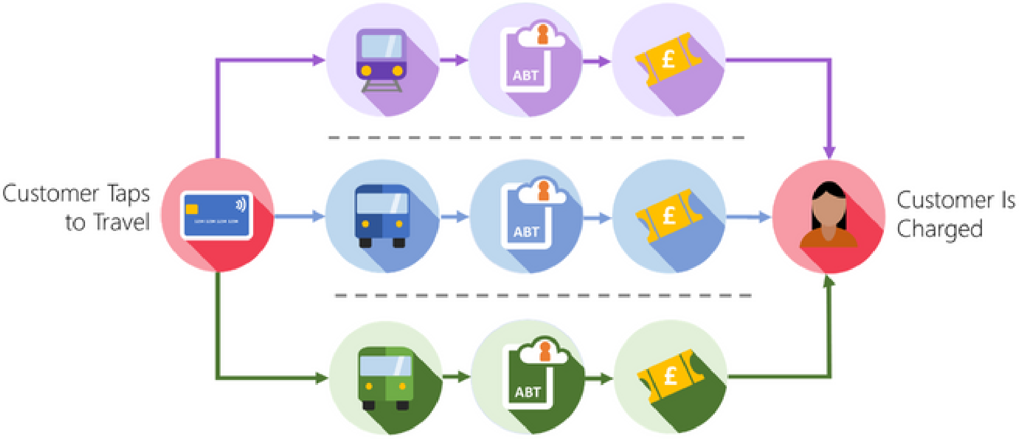


Figure 1: Existing Operator Solutions charge independently

Multi-operator / multi-modal projects in development

In response to the demand for multi-operator and multi-modal PAYG with capping (which has been requested by multiple Local Transport Authorities) there are a number of initiatives underway:

1 - The Bus Broker / Project Coral

The larger Bus Companies are currently in discussions regarding how to deliver multi-operator capping on Buses. Working closely with Transport for the West Midlands, these discussions focus on implementing a “Broker”, that will integrate with the ticketing back office of each of the participating Operators and identify if the customer has reached a multi-operator cap and instruct one of the back offices to charge the customer for the multi-operator cap value.

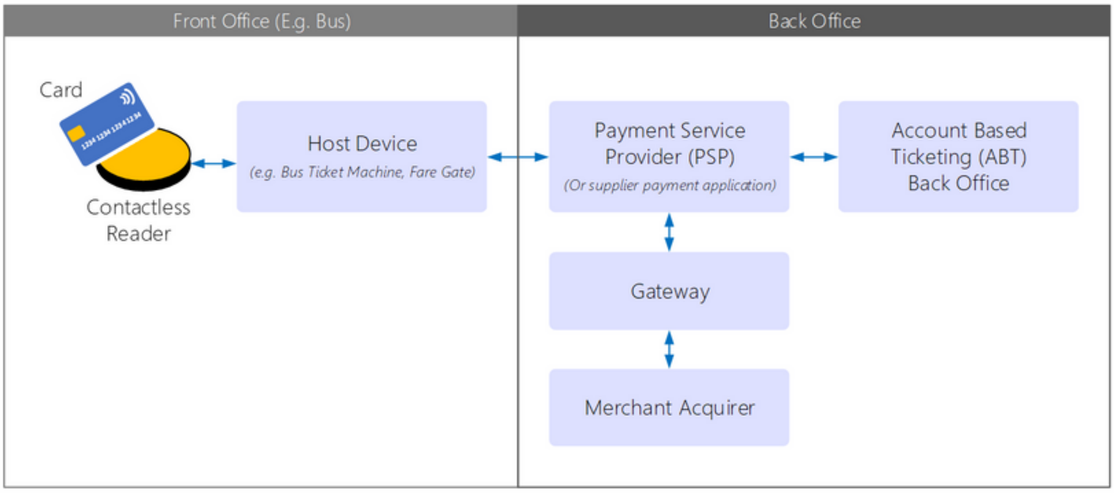
2 - Regional PAYG with Capping on UK Rail

Great British Railways transition team (GBRTT) and Rail Delivery Group (RDG) are investigating approaches for how to deliver regional PAYG on Rail, and how to work with regional Local Transport Authorities to support them in their ambitions to deliver multi-modal PAYG in their regions. This has been confirmed via the devolution deals in Greater Manchester and the West Midlands recently.

Protecting Payment Card Data

The key challenge to delivering multi-operator/modal PAYG ticketing using contactless payment cards (cEMV)

Existing Contactless PAYG schemes are delivered using a number of different ticketing supplier solutions. These are complex systems connecting readers on validation devices to back-office components responsible for managing payments (Payment Application / Payment Service Provider) and processing the Operator Fare Rules (ABT Back Office):



Front Office (E.g. Bus)
Back Office
Card
Contactless Reader
Host Device
(e.g. Bus Ticket Machine, Fare Gate)
Payment Service Provider (PSP)
(Or supplier payment application)
Account Based Ticketing (ABT) Back Office
Gateway
Merchant Acquirer

Figure 2: Common anatomy of a contactless PAYG system

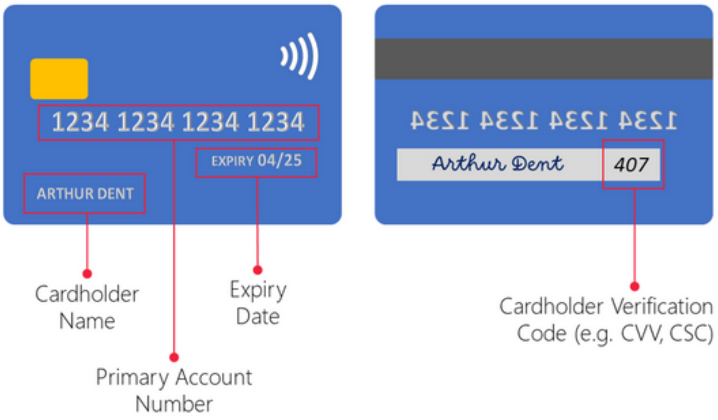
Whilst Multi-Operator ticketing schemes could be achieved by Operators all implementing the same ticketing solution, Operators have already invested in their existing solutions, and there is no mandate nor business case for the investment that would be required.

As such, any attempt to create a multi-operator, multi-modal ticketing scheme will require that these existing ticketing systems interface with each other or a multi-modal back office, enabling them to share customer journey and charge data so that it can be determined if the customer would benefit from a multi-modal/operator product or Cap.

Customers are using their bank cards to travel, and so each system needs to be able to consistently identify a customer's unique card when they share data, whilst also protecting the Cardholder Data in a manner that satisfies payment industry standards.

What is Cardholder Data?

The PCI security council considers the following data as "Cardholder Data", and in scope of PCI Compliance:



The Importance of Protecting Cardholder Data

Transport Operators that accept contactless payment cards have a responsibility to ensure that customer cardholder data is secured in order to:

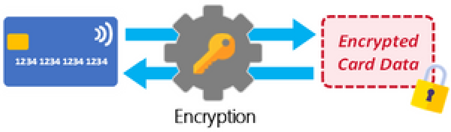
- Protect customers from fraudulent charges
- Protect suppliers and operators from significant fines and reputational damage caused by cardholder data breaches

Transport ticketing system suppliers design their end-to-end solutions and processes to meet the Payment Card Industry Data Security Standards (PCI DSS), which describe how cardholder data should be protected throughout the entire Solution.

How do ticketing systems protect cardholder data?

There are two main mechanisms suppliers use to protect Cardholder Data in ABT Ticketing Systems:

Reversible Encryption

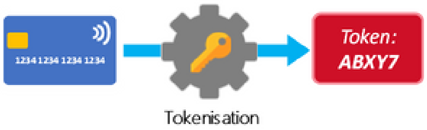


Incryption uses a key to cryptographically secure or "lock" cardholder data, so that only those parties in possession of the key can access it.

Encryption is reversible, enabling the encrypted data to be decrypted to allow access to the cardholder data.

Encryption is used to secure cardholder data for transmission between systems/parties.

Tokenisation (Hashing)



Tokenisation is the process of taking sensitive cardholder data and converting it into a non-sensitive equivalent identifier or "Token".

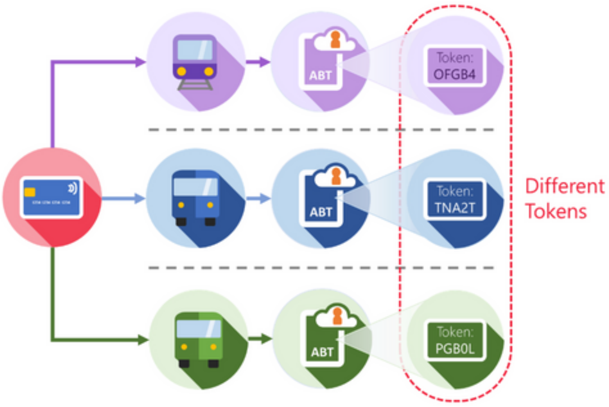
Tokenisation uses one-way encryption process called "hashing", meaning that it is not possible to turn the Token back into the Cardholder Data.

Tokenisation is used to generate a non-sensitive card proxy (a hash) to enable onward processing without using the card data

Tokenisation and the barrier to integration

Of these mechanisms, it is Tokenisation that is important in enabling multi-modal/operator PAYG with Capping. Tokenisation generates the identifier that each ABT Back Office uses to identify and process a card.

Currently, each Operator/Modal ABT Back Office system generates its own Token, and each back-office token will be different, even if the original card being Tokenised is the same. This is because each back office uses different Tokenisation Mechanisms or "Tokenisation Key ":



Implementing multi-modal/operator ticketing requires that ABT Back Offices share customer journey and charge information in order for a multi-model/operator product or cap to be identified.

Given that Cardholder Data cannot be safely shared, a new solution is required to create a consistent way of identifying a customer's payment card that will be understood by each ticketing back office.

The "Universal Transport Token"

The key to enabling multi-operator/modal PAYG

Given the maturity of existing contactless PAYG systems, it is not reasonable to ask that each participating ABT Ticketing Supplier changes the Token that their exiting ABT Back Office uses. Any such change would require significant changes to historic data, account data, payment partner data, and poses data integrity risks.

Instead, the generally accepted approach to enabling integration is to generate a new Token for each card, a "Universal Token" that is used exclusively for the sharing of cardholder data with other ticketing systems. This also meets PCI DSS best practice in that it proposes a different Token for a specific use rather than using the same Token for multiple purposes.

It is anticipated for any solution that enables communication between back offices such as a Bus Broker would require a new service that would manage "Universal Token keys", providing them to each participating Bus Operator's ticketing supplier.

Each supplier would generate the Universal Token in addition to their current ABT back-office Token. This would provide the common card ID that each Supplier would need to integrate with a Broker

This would enable a Bus Broker to identify if a multi-operator bus cap has been hit and, given that charging must be performed by an operator that has seen and authorised the card in that day, will inform which Bus Operator to charge for that cap (required because only an operator who has validated a card and performed an authorisation with the card issuer can request a payment).

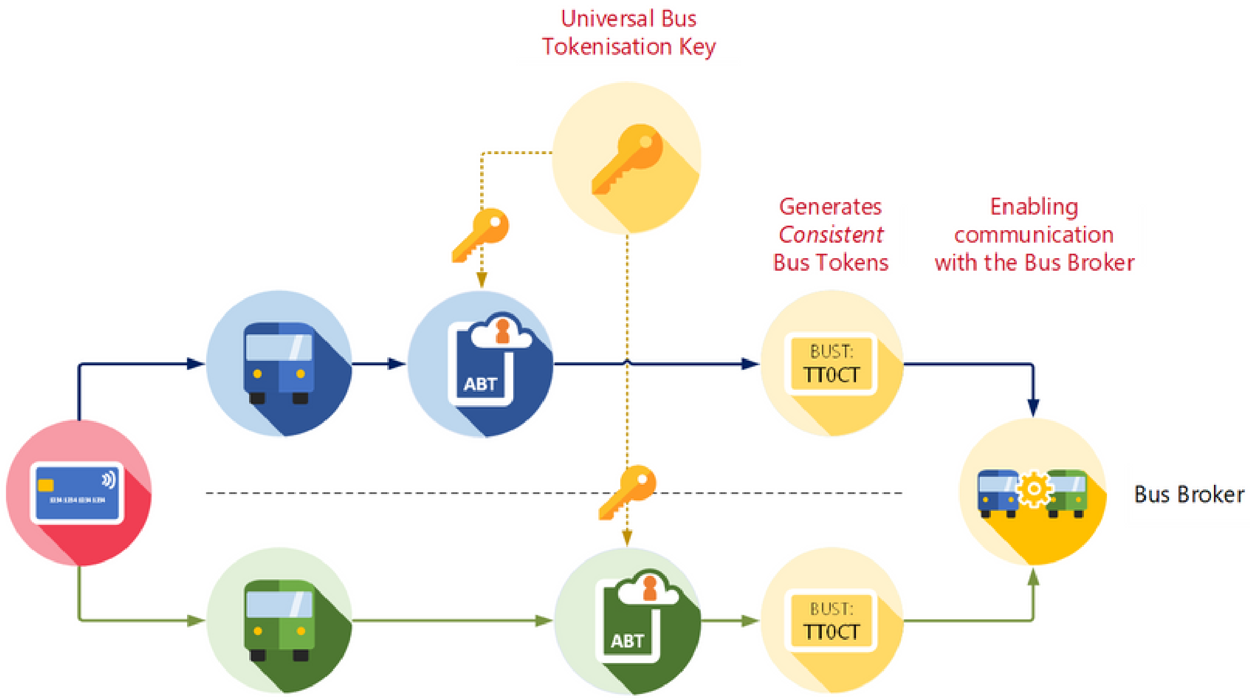

Universal Bus Tokenisation Key
Generates *Consistent* Bus Tokens
Enabling communication with the Bus Broker
ABT
BUST:
TT0CT
ABT
BUST:
TT0CT
Bus Broker

Figure 3: Bus Broker - Enabled by the Universal Bus Token

The risk of not coordinating Tokenisation in developing multi-modal initiatives

Currently, there is no formal technical collaboration between the Bus Broker initiative, the Rail PAYG initiative, or regional smart ticketing initiatives such as being discussed and developed in Liverpool, Scotland or Wales.

Whereas it is right that these initiatives should be able to progress at their own pace, there is a risk that in not considering the potential for a Universal Transport Token that is consistent across all Operators. Modes and Transport Agencies from the outset, stakeholders will unwittingly make later multi-modal integration significantly more technically challenging, with increased risk and significantly increased cost.

Modal or Regional Transport Tokens vs a Universal Transport Token

Should the Bus and Rail modes develop their plans independently, there is a risk that different solutions for the sharing of cardholder data will be implemented to support them, each performing the same function, but only enabling the sharing of cardholder data for a single mode or region (e.g., a Universal Bus Token solution, Universal Rail Token solution, and potentially Regional Token solutions required to enable regional schemes such as Liverpool or Manchester).

Each of these different Modal or Regional Tokens would need an entity to own the Tokenisation mechanism, and potentially to process multi-modal/operator rules. This risks creating multiple layers of "broker-like" components that would add significant unnecessary complexity and cost when attempting to integrate with other systems.

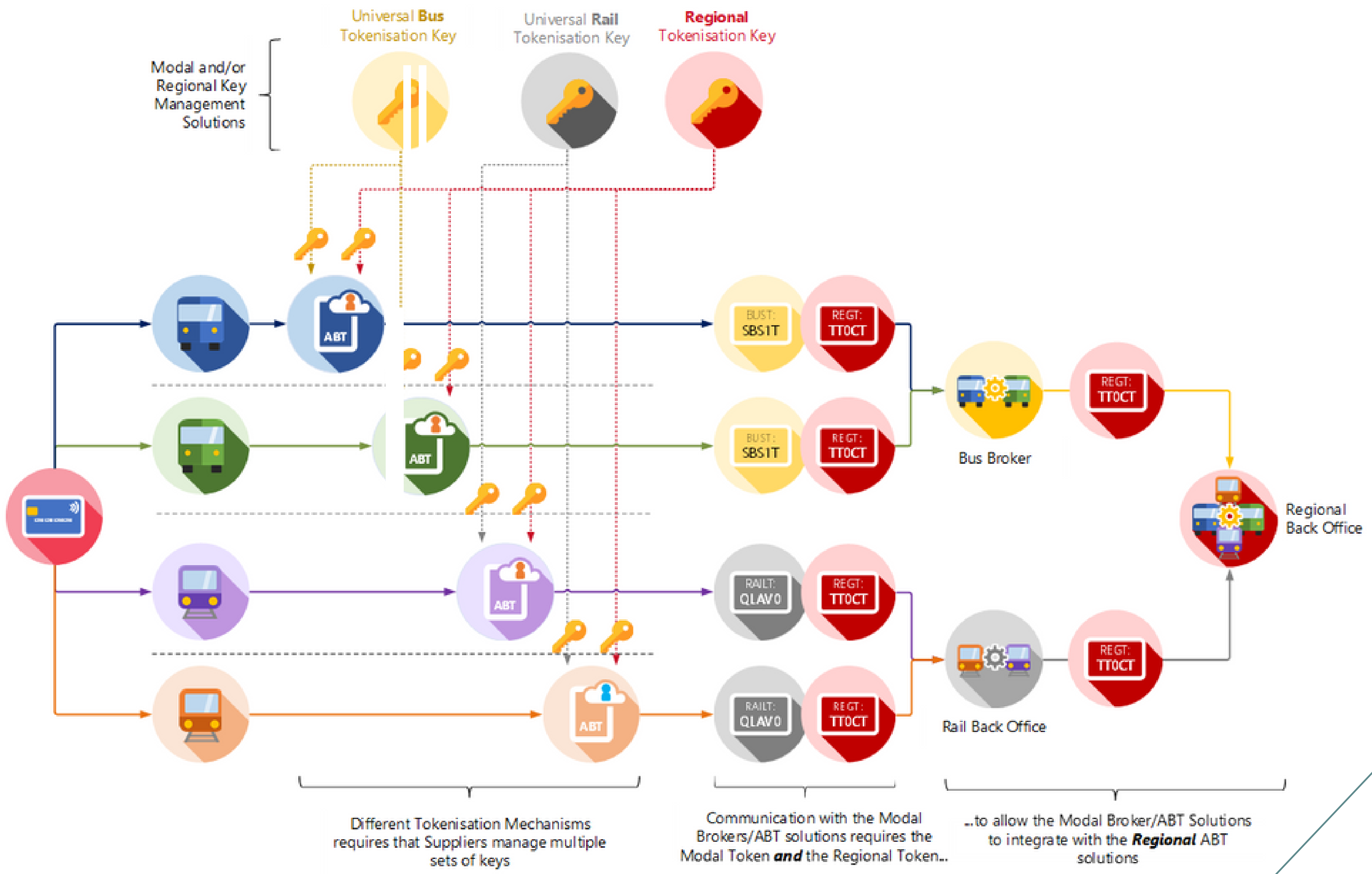
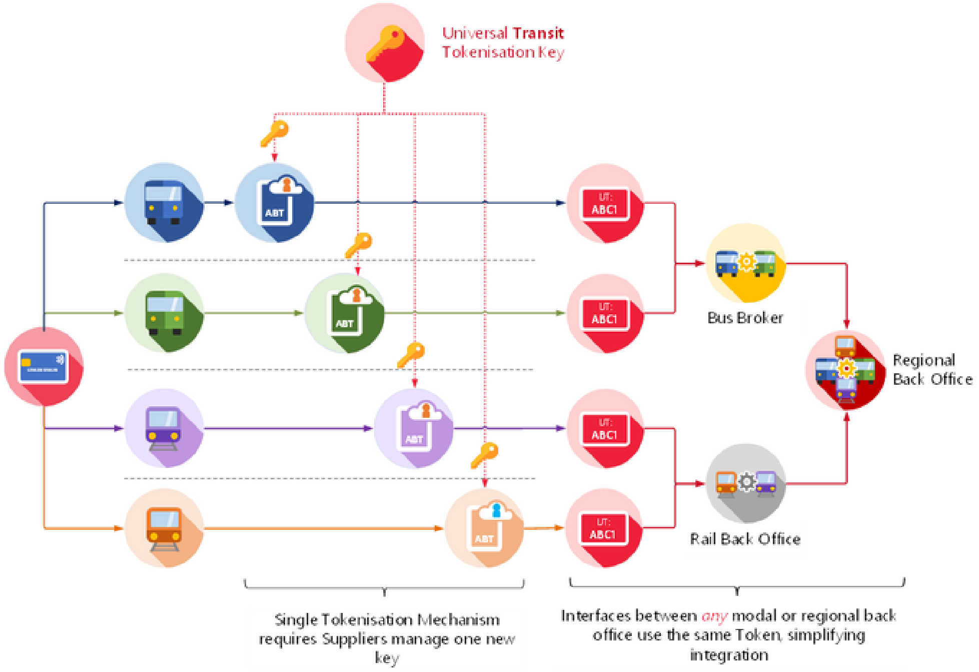

Modal and/or Regional Key Management Solutions
Universal Bus Tokenisation Key
Universal Rail Tokenisation Key
Regional Tokenisation Key
ABT
ABT
ABT
ABT
BUST: SBS1T
BUST: SBS1T
RAILT: QLAV0
RAILT: QLAV0
REGT: TT0CT
REGT: TT0CT
REGT: TT0CT
REGT: TT0CT
REGT: TT0CT
REGT: TT0CT
Bus Broker
Rail Back Office
Regional Back Office
Different Tokenisation Mechanisms requires that Suppliers manage multiple sets of keys
Communication with the Modal Brokers/ABT solutions requires the Modal Token ***and*** the Regional Token..
..to allow the Modal Broker/ABT Solutions to integrate with the ***Regional*** ABT solutions

Figure 4: Multiple Tokens - Layers of Tokenisation, complexity, and cost

The previous diagram highlights the complexity of requiring multiple token mechanisms to enable back offices to communicate. Whilst such a solution might be technically possible, it comes with the cost and risk associated with complex integrations that have been blockers to many integrated transport initiatives, and they could easily result in delivery of multi-modal ticketing solutions to be considered "too hard". Considering a consistent and standardised approach to Tokenisation can help avoid existing projects finding themselves facing this sort of solution when they turn their attention to multi-modal/operator propositions.

Instead, if a single universal solution for Tokenisation was used, generating a "Universal Transport Token", that Token could be used by any modal or Operator ticketing solutions to integrate with each other, or a regional ticketing solution


Universal Transit Tokenisation Key
ABT
ABT
ABT
ABT
UT: ABC1
UT: ABC1
UT: ABC1
UT: ABC1
Bus Broker
Regional Back Office
Rail Back Office
Single Tokenisation Mechanism requires Suppliers manage one new key
Interfaces between any modal or regional back office use the same Token, simplifying integration

This greatly simplifies complexity of integration between ticketing systems.

There is therefore a significant benefit for these parties to work together at an early stage to agree the approach for Tokenisation, recognising that this is one small part of a solution that can be consistent and that need not slow down the development of any individual project (e.g. with the definition of complex interfaces etc.)

Benefits of the Universal Transport Token

→ PCI Compliant
Removes the need for ABT ticketing solutions to share sensitive cardholder data in order to enable multi-modal PAYG with capping.

→ Creates a standard
mechanism for identifying unique payment cards in transport ticketing systems

→ Simplifies integration
between modal or regional Back Offices. This approach could be adopted by the TfL solution to enable interaction with other regional back offices.

→ Future proofing
Solution is re-usable for integration of new PAYG modes and other transport solutions (e.g., micro mobility, mobility as a service (MaaS))

→ Reduces Tokenisation effort and cost
Each Tokenisation Supplier involved in a multi-modal/operator solution would mean incremental effort to manage, and transaction costs associated with generating and storing multiple tokens for the same card.

→ Reduces supplier integration effort and cost
Reduces the amount of work each individual Operator's ticketing solution supplier has to do to maintain multiple Operator and/or regional keys.

Limits coordination required between projects/schemes

Limits the amount of coordination and agreement that is required between active or developing projects to the minimum possible. Requires only that the Tokenisation solution is agreed between all parties, does not require any delays caused by parties having to agree to a wide range of business rules or interface standards.

Simplifies Management of the Keys

Enables a single entity to manage and track use of the Universal Transport Token, simplifying the process for triggering key roll; generating and distributing new keys to maintain security.

Simplified Customer Support Processes

The Universal Token can be shared between systems not just for payment use cases, but also to identify the customer for the purposes of customer support. This removes customers support processes from PCI DSS scope.

Drawbacks of the Universal Transport Token

→ Requires Agreements
Requires agreement between the existing projects currently working on implementing contactless PAYG propositions. Many of these projects are early in development and so may not have considered the approach to tokenisation yet, whereas others may have already decided on a solution, and to change the current approach to Tokenisation may result in additional cost or delays to their current project.

→ Reliance on a single Tokenisation Supplier
The Universal Transport Token approach relies on a single supplier to manage the keys used for any interoperable ticketing scheme, reducing competition in providing tokenisation services.

→ "Ownership" of the Tokenisation Mechanism
Requires a single party to "own" the universal Tokenisation mechanism, leading interaction with the supplier regarding development, maintaining security, coordinating with the various parties that seek to use it etc.

→ Increases Risk
Technically, the more uses of a key (either one party uses it lots of times, or multiple parties using less often but in aggerate lots), the easier it is to decipher the key. In addition, the greater number of parties using the key, the more prevalent it is and the more individuals and systems have access to it, the greater the risk and impact of the key being compromised. This is however mitigated by the following:

Increases Risk

Technically, the more uses of a key (either one party uses it lots of times, or multiple parties using less often but in aggerate lots), the easier it is to decipher the key. In addition, the greater number of parties using the key, the more prevalent it is and the more individuals and systems have access to it, the greater the risk and impact of the key being compromised. This is however mitigated by the following:

- This approach simplifies management of the Universal Token Keys, so it is easier to track key usage and roll the keys more frequently in order to reduce the chance of the key being compromised

- The Universal Transport Token Key is only used to communicate between back-office ticketing systems or PSPs. As such it need not be provisioned to individual devices, limiting exposure of the keys and chance of compromise

- Processes, mechanisms and systems to ensure that the keys are transmitted and stored securely to minimise risk of disclosure

Transport for the North
2nd Floor
4 Piccadilly Place
Manchester
M1 3BN

0161 244 0888
info@transportforthenorth.com

TRANSPORT FOR THE NORTH

transportforthenorth.com