Assurance and Audit Committee

Date: **17 December 2014**

Item: **Contactless – Security Controls in Place to Protect Payment Card Data**

This paper will be considered in public

1 Summary

1.1 At the meeting of the Audit and Assurance Committee on 8 October 2014, Members requested a report on data security and contactless payments. This paper articulates the security controls built within the Contactless system, the compliance position against the main applicable standards and certifications, the validation activities that were conducted with the banking industry, and an understanding of the level of engagement established with banking entities and the Train Operating Companies (TOCs).

1.2 Since 2007, the introduction of new methods of ticketing at TfL has provided greater convenience to customers while also reducing the cost of revenue collection. Building upon the success of Oyster, TfL looked for other technologies that would support a more simplified process in which ticketing was less onerous to customers. A study in 2006, conducted with the help of the Massachusetts Institute of Technology (MIT), showed that contactless bankcards and mobile phones equipped with near field communication offered the best prospects. This work has since concentrated on contactless bankcards due to the slow pace of development in the mobile phone industry.

1.3 Contactless provides good customer experience as there is no need for the customer to buy a ticket or work out the cheapest combination of products for any combination of journeys. With Contactless, the only action required by the customer is to touch a bank card on the gate's reader and the system calculates the best fare for the combination of journeys and creates a daily charge for the card which is debited directly from the customer's bank account.

1.4 Building such an innovative product was challenging in many aspects and key questions had to be answered in the initial phase of the project. Although there are similarities in the way the Oyster and Contactless systems work there are also significant differences. It was essential to determine, for example, how to integrate payment applications in the reader without degrading performance times; what payment model should replace the retail model not suitable for transit; how to design a back office software delivering the required level of throughput for the execution of London's complex fares structure; and what security model should be established to provide optimum protection of Payment Card Data.

1.5 A paper is included on Part 2 of the agenda, which contains exempt supplemental information. The information is exempt by virtue of paragraphs 3 and 7 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to the

business affairs of TfL and action which might be taken in relation to preventions, investigation or prosecution of a crime.

2 Recommendation

2.1 The Committee is asked to note the paper.

3 Learning from Oyster

3.1 Oyster is a card centric system which means that the ticketing business logic such as Pay As You Go (PAYG) fare calculation is executed by the reader at the point of transaction. This architecture was driven by the technology constraints faced by the design team at the end of the 1990s where network infrastructure and back office servers capacity were not adapted for back office processing. Equally, with a prepaid purse it is not possible to verify quickly whether the account has money on it unless the purse balance can be read directly from the card. As a result, with Oyster, each reader is a billing engine which must calculate a price within 300 milliseconds in order to maintain gate throughput and bus boarding times required to support TfL operations.

3.2 The functionalities supported by the reader are very similar to those implemented in mobile phone operators' billing engines supporting PAYG price calculation. However, unlike these industries where one billing engine is implemented in the back office, Oyster supports more than 20,000 of them distributed across London. Managing changes across the system is complex because new versions of software have to be rolled out across all 20,000 readers.

3.3 The system also presents limitations hindering our ability to innovate. For example, the limited storage capacity of the card and the limited reader processing power would render impossible the implementation of Monday to Sunday capping with the current Oyster architecture.

3.4 The choices made in the design of Oyster have proved successful, with 11 years of successful operations. However the implementation of Contactless was an opportunity to take into account the limitation of Oyster and build a system that would not only accept these cards at the gate but also provide a platform for future innovation.

4 Contactless Use Cases

4.1 The key technical principle adopted at the early design phase of the project was to keep the reader simple and transfer as much complexity as possible to the back office. Only this type of architecture could support the agility required due to the innovative nature of this project and enable fast delivery of change.

4.2 Figure 1 provides a high level view of the Contactless system architecture to support the description of the three main use cases of the system: Pay for travel, After Care and Revenue Inspection.

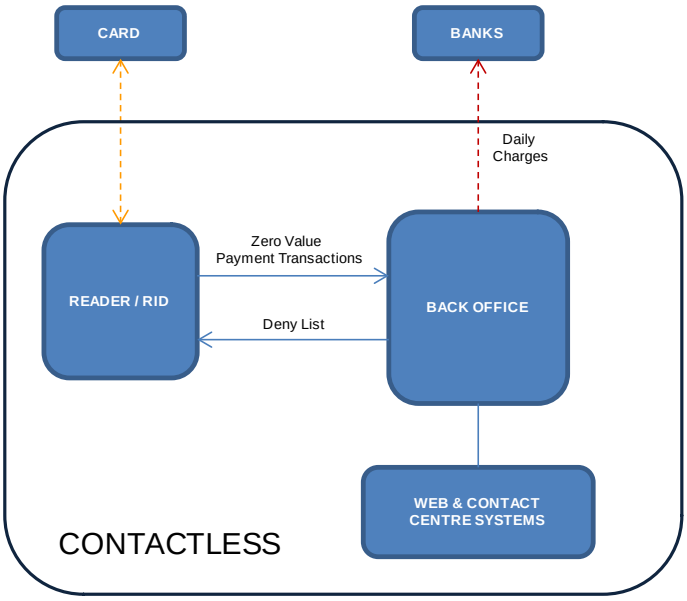

Figure 1: Contactless, a Back Office centric system

Pay for Travel

4.3 When travelling on the system using Contactless, customers are required to touch their payment card on the gate's readers to indicate the beginning and the end of the journey. Sometimes additional touches are necessary in the middle of a journey to indicate an interchange or mark a particular route.

4.4 Every time a card is presented, the reader authenticates the card and generates a payment transaction which is sent to the Back Office a few seconds later. Unlike Oyster there is no complex calculation taking place so the reader simply generates a zero value transaction.

4.5 The Back Office receives all transactions generated by customers to access the network and performs two main operations:

(a) During the traffic day, transactions received from the readers are immediately analysed to determine whether the card is eligible for travel. The assessment is based on the execution of risk management rules defined in the Transit Transaction Model (TTM). If the card is not permitted on the network then the card number is added to a central file called the Deny List. A new version of the Deny List is distributed to all readers every 10 minutes. As a result, access to the network is denied the next time the card is presented to an entry gate, a platform or bus validator.

(b) At the end of the traffic day, the back office retrieves all transactions generated on the network for that day and triggers fares calculation. As illustrated on Figure 2, individual transactions are aggregated into one daily charge which is debited directly from the customer's bank account. The daily charge appears as one line item on the bank statement the following day.

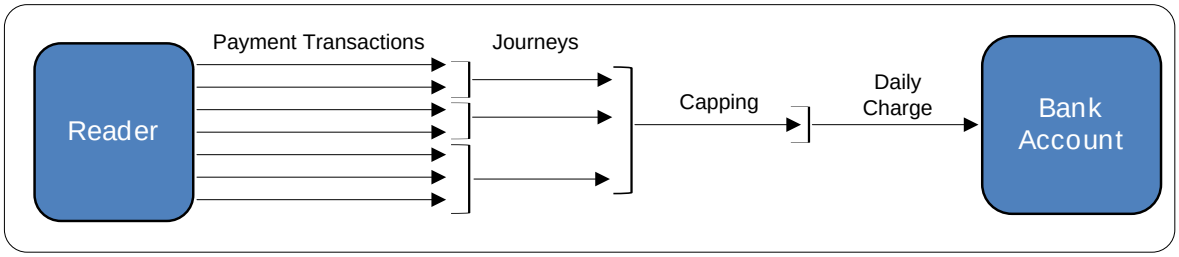

Figure 2: Back Office aggregation mechanism

After Care

4.6 The customer's bank account only shows one global charge for the day and does not provide any details of contributing journeys. However the customer can use the Contactless website for additional information and services. There are two levels of online services outlined below.

4.7 Customers can remain anonymous and access seven days of journey history without an online account. They simply need to enter their card number and billing address on the website. After validation with the card issuer, the system returns seven days journey history showing the daily charge incurred by the card, journeys and individual transactions. This provides the customer with complete transparency on charges applied to the card.

4.8 Alternatively, the customer can decide to create an online account and register his payment card for an enhanced online experience and access up to twelve months of journey history and charges, comprehensive breakdown of charges and journeys, and email notifications. Customers can also pay outstanding debts and make a refund application for incomplete journeys.

4.9 Customers can also contact TfL's contact centre if they require assistance. Contact centre staff can undertake a number of functions on behalf of the customer. They can for example modify account details, reset passwords, view the status of cards (denied or not), produce payment and journey history statements, issue refunds for incomplete journeys and clear outstanding debt.

Revenue Inspection

4.10 Because Oyster is a card centric system, key information stored on the card, such as the PAYG balance, attributes of season tickets or the last eight transactions, facilitates revenue inspection. Revenue Inspectors can read this information from the card using a specific device to identify the status of the card at any point of time and decide whether it is valid for travel. It wasn't possible to replicate this solution for Contactless because the system is not authorised to write any information on the card. Write access to the chip is protected with security keys managed by the bank and not distributed to third parties.

4.11 The Contactless revenue inspection process is based on the ability or not of the Revenue Inspector to identify whether the card was validated on a reader before travelling on the system and by the presence or not of the card on the Deny List.

4.12 The Deny List is distributed to all Revenue Inspection Device every ten minutes and is a key input to determine whether the card is eligible for travel for both rail and bus inspections. In addition a Revenue Inspection transaction is generated by

the device after each inspection and sent to the back office for processing and analysis.

4.13 Before starting inspection on a bus, the Revenue Inspector is required to touch the Revenue Inspection Device (RID) on the bus reader. The device retrieves and stores all card validations made on the reader for the current trip. The Revenue Inspector can then proceed with the inspection and use the RID to read the cards presented by customers. The RID reconciles the card number with the list retrieved from the reader and checks if the card is on the Deny List.

4.14 On rail the validity of the card is determined in the Back Office by reconciling revenue inspection transactions with reader transactions. The card is only declared invalid at the moment of inspection if it features on the Deny List.

Definition of the Transit Transaction Model (TTM)

4.15 The TTM is a new Contactless payment model established by TfL in collaboration with Visa, MasterCard and American Express. It has been designed to support operational constraints of transit environments and joins the worlds of transit and payment together. The TTM is now mandated on all card issuers worldwide by Mastercard and Amex and in Europe by Visa Europe. TfL's implementation of the TTM is the first and so far the only example of this, which makes TfL's intellectual property on this particularly valuable.

4.16 The need for a TTM arose as the way Contactless cards are used in the retail environment is not suitable for the transit environment due to two critical differences between retail and transit. First, the value of the payment is not known in transit at the time of using a Contactless card on rail; it only becomes known when a journey has been completed, with two or more touches of a Contactless card. Second, the methods to control risk in the retail environment require the card to default to Chip and Pin from time to time, which cannot be supported in the high intensity transit environment.

4.17 The TTM includes a detailed set of rules agreed with the Card Schemes by which the system must operate for risk management and debt recovery functions. Further information is provided in the paper on Part 2 of the agenda.

4.18 The TTM is executed in the Back Office and outputs are communicated to readers via the distribution of the Deny List.

5 System Architecture Overview

5.1 Figure 3 provides an overview of the Contactless architecture, representing the main components involved in the processing of Contactless transactions. The system was built to separate the payment processing function from the business logic implementation, which presents two significant benefits.

5.2 Containing payment processing to a small number of components limits the propagation of payment card data across the system and therefore limits the exposure to the risk of payment card data loss. This also reduces the scope of payment standards and regulation, and limits the constraints on the overall system.

5.3 The second benefit is that the business logic is executed against a token and is therefore dissociated from the ticketing medium, providing greater flexibility for future evolution.

5.4 Interactions with the payment systems are based on standardised interfaces that have been certified against EMV protocol for card reader interface and ISO8583 for the interface between the Payment Gateway and the banks back office systems. The EMV card reader interface contains a very high degree of encryption and has never been compromised.

5.5 Additional information is included in the paper on Part 2 of the agenda.

6 Security Artefacts

6.1 In designing the Contactless system the key objective was to limit the distribution of payment card security data (PCSD) across the system and implement robust security controls to protect PCSD within the payment processing area.

6.2 A number of encryption and tokenisation techniques are used to segregate the data into confined areas and to secure them within those areas. Additional information is included in the paper on Part 2 of the agenda.

7 Compliance Framework

7.1 The purpose of this section is to provide an overview of system compliance with the payment security standards mandated by the PCI council, the Card Schemes (Visa, MasterCard and American Express) and the Acquirer (Barclays).

7.2 The implementation of systems and interfaces according to specifications and security standards mandated by the Card Schemes and the Acquirer is validated by compliance to the following:

(a) **Card/Reader Interface:** Compliance with standards set up by the card schemes.

(b) **Payment Gateway/Banks systems Interface:** Accreditation with the merchant aquirer.

(c) **Reader Payment Software:** Compliance with standards set up by the card schemes.

7.3 The main challenge in the application of PCI DSS to the Contactless system was to define where the standard should apply. As it was designed for the retail environment and not for the type of payment architecture implemented for Contactless. New standards have therefore been developed, working with the payments industry, for implementation of PCI DSS rules in the transit environment.

7.4 Additional information is included in the paper on Part 2 of the agenda.

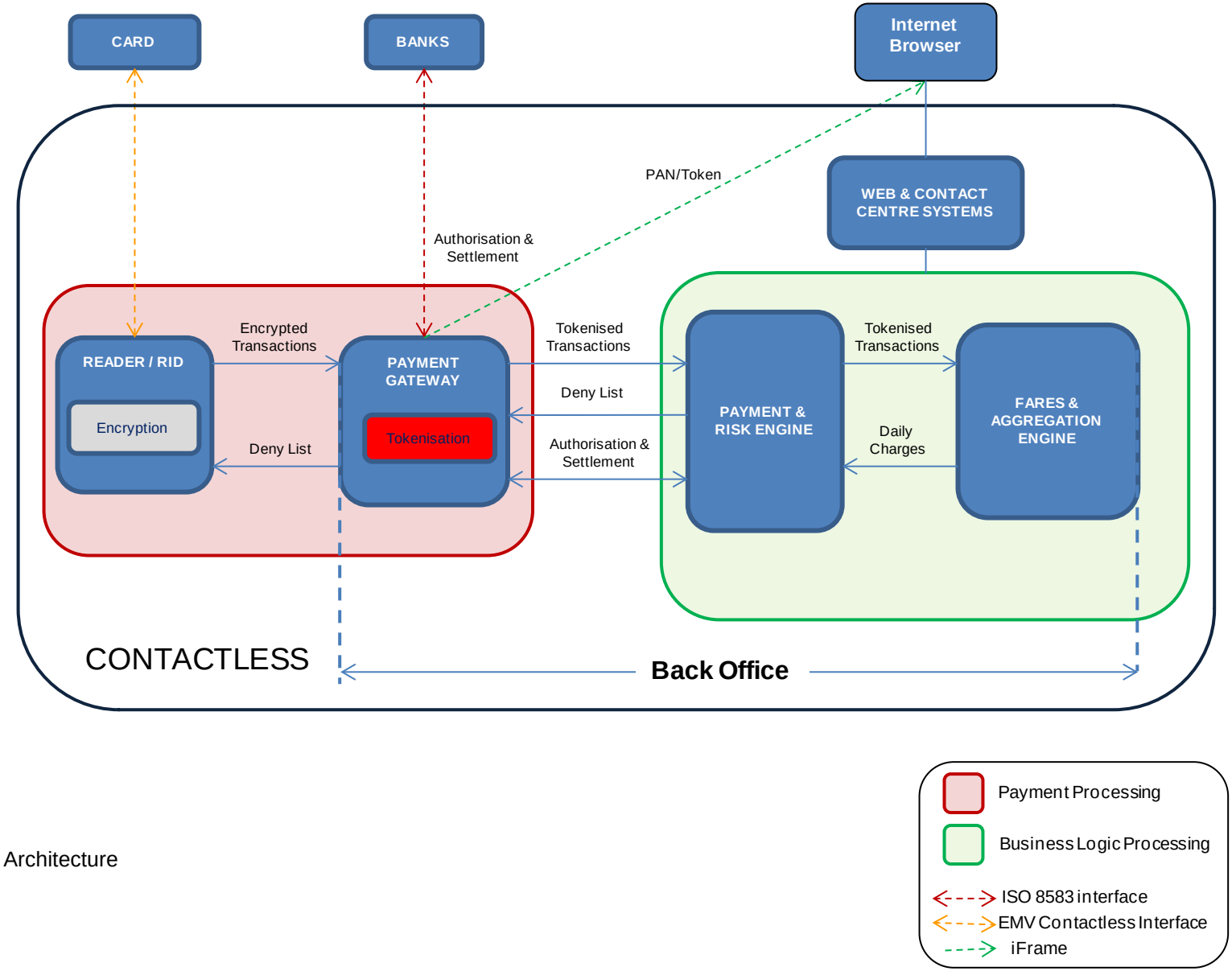

Figure 3: High Level Architecture

8 Third Party Interfaces

8.1 A security working group was established by TfL at the beginning of the project to involve all interested parties during the design and implementation of the security model and ensure common understanding of the controls strategy and implementation. It includes representatives and experts from TfL, Cubic, Visa, MasterCard, Barclays, NCC (QSA), Consult Hyperion.

8.2 For contactless acceptance, TfL's relationship with the TOCs is an extension of that agreed for Oyster pay as you go. This means that TfL is the operator of the scheme and the owner of all equipment andthis arrangement means that all the security design features described in this paper are implemented by TfL in exactly the same way for TOCs.

8.3 Additional information is included in the paper on Part 2 of the agenda.

9 Financial Implications

9.1 The implementation of Contactless was previously approved by the Finance and Policy Committee in 2011 and has cost £66m. Savings are expected against this through a reduction in commissions paid on ticket sales and other sources.

9.2 In the first two months of Contacless, acceptance on Tube and rail services demand for this new form of ticketing has grown steadily. Ten per cent of all pay as you go journeys are now being made using Contactless cards.

List of Appendices:

Exempt supplemental information is included in a paper on Part 2 of the agenda.

List of Background Papers:

None

Contact Officer: Shashi Verma, Director of Customer Experience
Number: 020 3054 0709
Email: shashiverma@tfl.gov.uk