Audit and Assurance Committee

Date: **16 June 2015**

Item: **Contactless – Security Controls Update**

This paper will be considered in public

1 Summary

1.1 The use of Contactless Payment Cards to pay for travel across all modes of TfL was launched in September 2014. The use of Contactless since launch has risen steadily to more than 700,000 journeys per day and a cumulative total of 98 million journeys equating to over £200m in fares collected as of mid-May 2015.

1.2 At the Audit and Assurance Committee meeting on 17 December 2014, the Director of Customer Experience presented a paper on the development and implementation of the security controls on the TfL Contactless system to protect Payment Card Sensitive Data (PCSD). The purpose of this paper is to provide an overview and update on those security controls in place since the launch of Contactless.

1.3 This paper will cover six key control areas:

(a) PCI-DSS Audit;

(b) Card Data Environment Physical Security;

(c) Card Data Environment IT Security;

(d) Operational Support System;

(e) Information Security Forum; and

(f) Standards Compliance Framework.

1.4 In summary, all controls are operating fully to expectations and compliance has been maintained against all applicable standards on the Contactless system.

2 Recommendation

2.1 The Committee is asked to note the paper.

3 High Level Architecture

3.1 Figure 1 provides an overview of the Contactless system architecture, representing the main components involved in the processing of Contactless transactions.

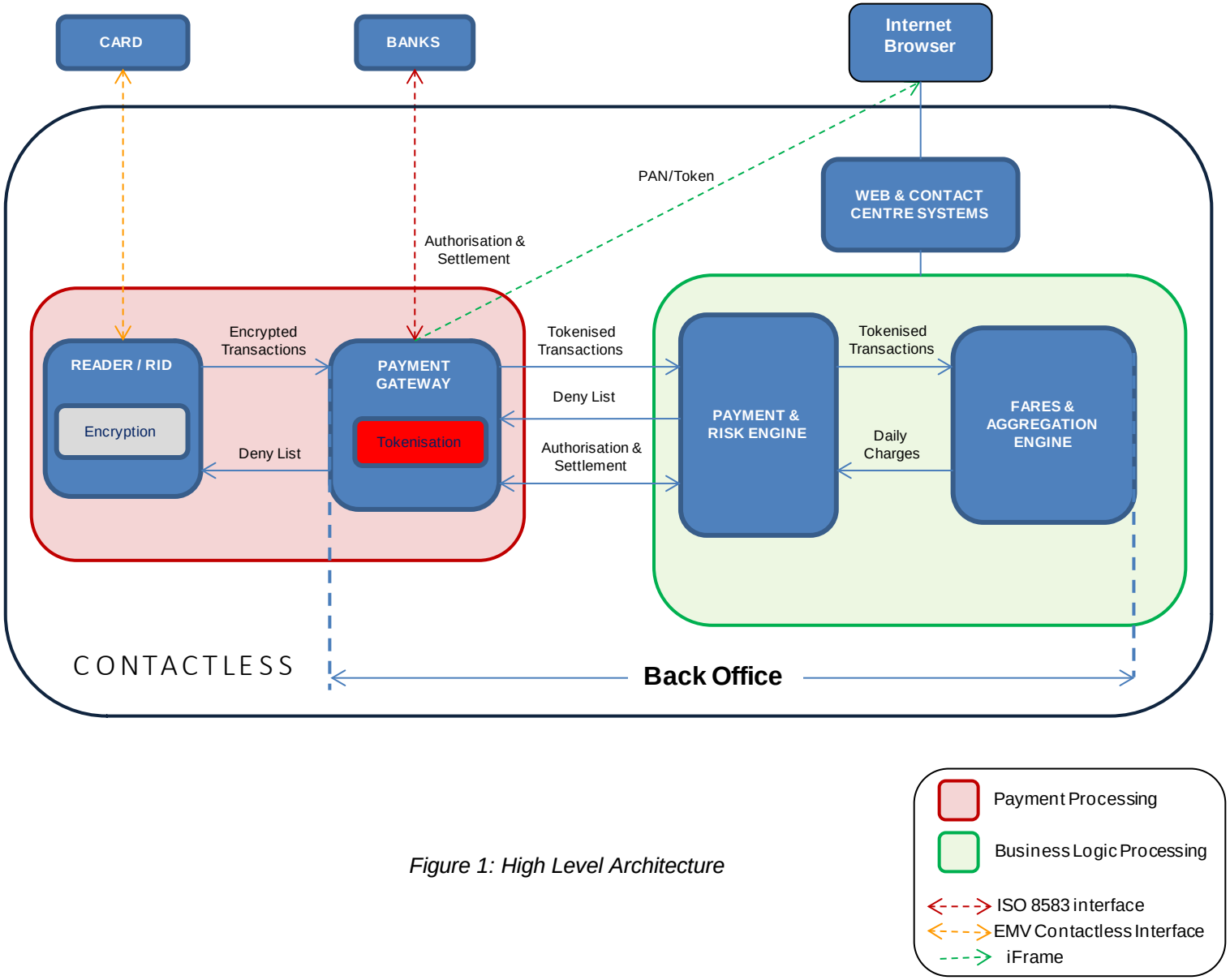

Figure 1: High Level Architecture

3.2 As detailed in the paper submitted to the 14 December 2014 meeting, the system was designed and built to separate the payment processing functions from the business logic implementation, which significantly reduces the risks of payment card data loss and increases flexibility for future developments.

3.3 Payment Card Sensitive Data is contained within the payment processing zone highlighted in red in Figure 1 and not distributed across the business logic components which are highlighted in green.

3.4 Interactions with the payment systems are based on standardised interfaces which 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 high degree of encryption and has never been compromised.

4 PCI-DSS (Payment Card Industry – Data Security Standard) Compliance

4.1 The payment processing zone is subject to an annual external audit by a Qualified Security Assessor (QSA) which is a company certified by the PCI Council to perform such audits.

4.2 Customer Experience instructs NCC Group as its QSA to perform the audit for PCI-DSS compliance on the Contactless system. The most recent Report on Compliance (ROC) was issued on 23 December 2014.

4.2 The scope of the audit includes identifying and reviewing all channels and locations which are used to process payment transaction data. In addition to reviewing cardholder data flow and network designs, NCC conducts physical examinations and testing of the cardholder data environments within the data centres which are used by Cubic Transportation to provide the Contactless system. They also review the policies and procedures in place to manage the system and interview personnel from all relevant teams (the Security Team, Network Team, Development Team, Wintel and Server Team, Back Office Systems Team, Human Resources Team and Quality Assurance Team).

4.3 The output of the audit is a compliance certificate in the form of a Report on Compliance which details all the audit activities, the devices and networks tested, and compliance against each separate requirement of the PCI-DSS standard.

5 Card Data Environment Physical Security

5.1 The Card Data Environment (CDE) is hosted within high security data centres[1]. Both data centres are rated Tier III which means that they meet required standards for security and redundancy. For example, all IT equipment must have dual power and cooling with a minimum availability of 99.98 per cent year round.

5.2 The physical security at each data centre includes:

(a) Security Operations Centre manned 24x7x365;

[1] The location of these centres was removed following publication.

(b) Security guards on patrol 24x7x365;

(c) Constant recorded CCTV surveillance of all internal/external common areas;

(d) Intruder alarms in all areas;

(e) Automated intrusion detection system;

(f) Mantrap access for all personnel; and

(g) Access control via security cards and biometrics.

6 Card Data Environment (CDE) IT Security

Zoning of CDE

6.1 Each hall within the data centres containing the CDE is protected by a secure entrance with its own internal mantrap. Once inside, the halls are divided into different zones separating equipment performing different functions and by security levels. The equipment performing the payment processing functions is held in the highest security area.

Firewalls

6.2 There are three sets of firewalls which protect the Card Data Environment. Each firewall is comprised of hardware and software from different market leading vendors which form a set of concentric barriers with the equipment containing PCSD at its centre.

CDE SecurityTools

6.3 The servers and devices within the CDE contain numerous IT tools which perform essential security functions including:

(a) Firewalls;

(b) Intrusion detection and prevention;

(c) Event logging and management;

(d) Database monitoring;

(e) Anti-malware;

(f) Security scanning;

(g) Change detection; and

(h) Remote access authentication.

7 Operational Support System ("OSS")

7.1 The OSS is a customised tool which monitors the Contactless system and is staffed around the clock by teams at Cubic and Customer Experience. A part of this monitoring includes automatic status updates which are sent from the card readers to the OSS every 5 minutes. Alerts are picked up by the Cubic service teams for appropriate remedial action.

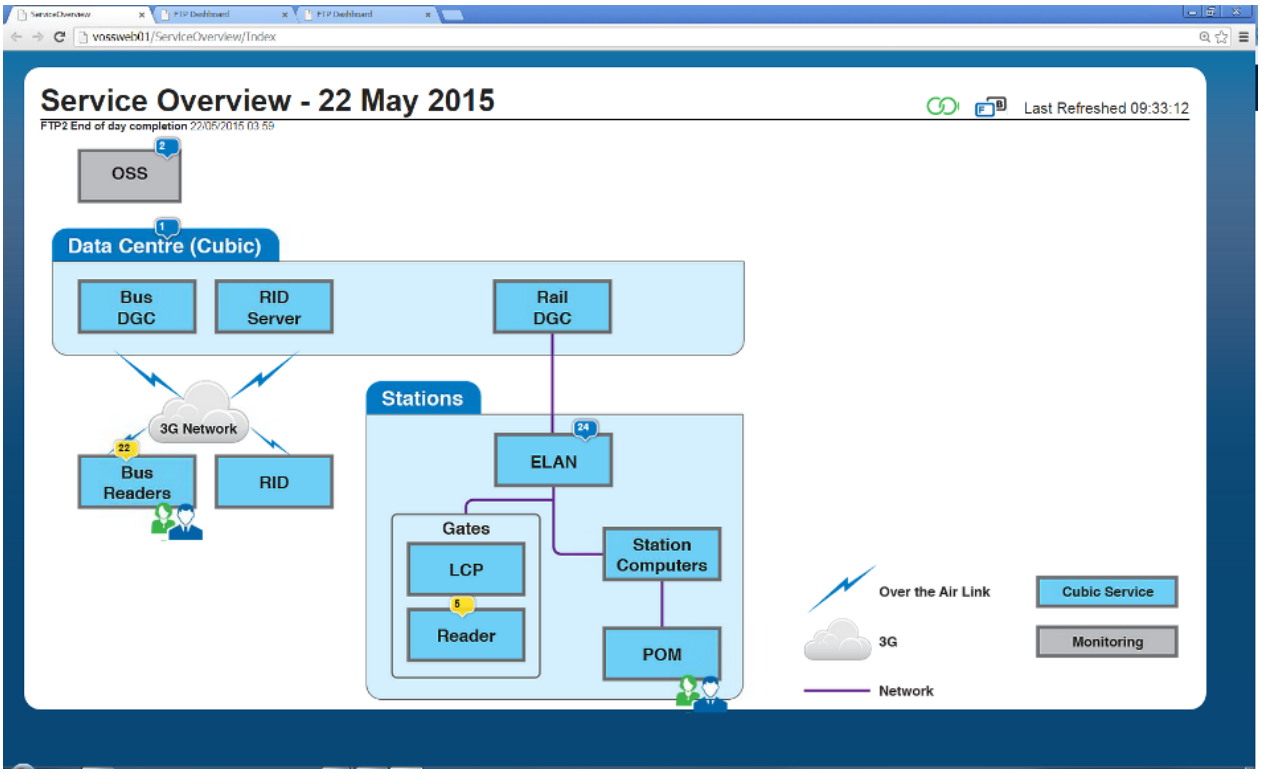

Figure 2: Operational Support System Overview

8 Information Security Forum

8.1 The Information Security Forum (ISF) is a management group consisting of senior managers from Cubic Transport and Customer Experience who meet monthly to discuss security issues. The composition of the group includes security managers, heads of IT and engineering, network and architecture managers, service managers and commercial managers.

8.2 The activities of the ISF include reviewing security reports and any new incidents, as well as discussing upcoming activities such as auditing, patching and security upgrades.

9 Standards Compliance Framework

9.1 The 17 December 2014 paper detailed the compliance framework which applies to the Contactless system, including mandated security standards which apply to the card readers, the Payment Gateway and the reader payment software.

9.2 Customer Experience continues to work with the PCI Council, the card companies, Barclays Bank and external consultants and auditors to ensure that compliance against all applicable standards is maintained.

10 Legal Implications

10.1 As the operator of the system, the legal obligation to maintain PCSD security remains with TfL. As the primary contractor delivering the fares payment system, Cubic Transportation is under stringent contractual obligations to maintain the security of the system and to ensure that these obligations are flowed down to its own subcontractors. These obligations include strict requirements for minimum levels of service for monitoring, reporting and resolving issues.

11 Financial Implications

11.1 The implementation of Contactless has cost £66m against which savings are expected through the reduction in commissions paid on ticket sales and other sources. To mid-May 2015, the Contactless system has collected over £200m in fares and the use of the system is expected to continue to grow.

List of appendices to this report:

There are no appendices to this report.

List of Background Papers:

Audit and Assurance Committee Paper:
Contactless – Security Controls in Place to Protect Payment Card Data, 17 Dec 2014

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