Transport for London
London Taxi and Private Hire

Guidelines for Electronic Payment Devices, including processing payments using Mobile Equipment/Devices in licensed London Taxis & Private Hire Vehicles.

Introduction

From 1 January 2017 every licensed London taxi must be equipped with a TfL approved card payment system. The card payment device must be correctly installed within the passenger compartment. TPH Notice 13/16 applies.

There are various card payment devices available on the market to provide solutions for the payment of taxi and private hire services. These guidelines set out to ensure that those electronic payment devices, such as pin entry devices, contactless payment systems (near field communications) and mobile devices, (smart phones, tablets, laptops, etc) used in London Taxis and Private Hire Vehicles (PHV's) licensed by Transport for London (TfL), meet the current banking security standards, payment transaction processes and protocols.

General Requirements

Applications for approval to use specific payment devices, including mobile device applications, must be made in writing to the Vehicle Policy Manager for Taxi and Private Hire at TfL.

Only payment devices and signage approved by TfL can be used in licensed vehicles and will be subject to the conditions of vehicle licensing. All payment devices must:-

- comply with the requirements of the current UK banking industry standards as stipulated by the Financial Conduct Authority (FCA).
- be listed on UK Finance (formally the UK Cards Association) website as an approved device.
- comply with latest release of the UK Finance approved guidelines relating to organisational security policies.
- comply with EU Payment Services Directive 2 (effective January 13th 2018).
- meet all requirements as regards safety, technical acceptability and operational/data integrity.
- be checked regularly and maintained to operational standards, including any repairs after damage.

- be designed, constructed, installed and/or carried in such a way and in such materials as to present no danger to passengers or driver, including impact with the equipment in the event of a collision.
- be protected from the elements, secure from tampering and theft and located such as to have the minimum intrusion into any passenger area, including designated wheelchair space, or impact on the luggage carrying capacity of the vehicle.
- be free from obscuring or interfering with the operation of any of the vehicle's standard and/or mandatory equipment, i.e. not mounted on or adjacent to air bags/air curtains or within proximity of other supplementary safety systems which may cause degradation in performance or functionality of such safety systems.
- comply with any legislative requirements in respect of the Motor Vehicle (Construction and Use) Regulations, 1986, in particular with regard to equipment obscuring the view of the road through the windscreen.

Automotive Electromagnetic Compatibility Requirements (EMC)

Any charging equipment used must not interfere with any other safety, control, electrical, computer, navigation, satellite, or radio system in the vehicle.

Information regarding type approval of the payment device or payment system will be required. The installed equipment should be clearly e-marked. If any electrical equipment is CE marked for EMC, a certificate will be required from an appropriate authority declaring that the equipment is non 'immunity-related' and suitable for automotive use, as part of the approval process.

Payment Device Functionality

All payment devices must:-

- meet all requirements and standards as stipulated by the card scheme companies in terms of connections to a host such as GPRS, 3G, 4G, bluetooth or other connection methods to complete payment transactions.
- links between a taximeter, card payment applications and other electronic devices must be in 'read only' format.
- provide functionality to protect the confidentiality of critical data (in particular PINs) whilst the card transaction is being processed.
- allow card details to be stored for the minimum amount of time required to enable the payment transaction to complete, thereafter card details must be deleted / disposed of in a secure manner.
- have the facility to produce printed receipts which comply with the current banking standards.

Payment Device Approval/Certification

The payment device/solution must comply with the following standards (as supplied in conjunction with UK Finance):-

- Transactional Smartcard Reader Protection Profile (TSRPP).
- Current Card Acceptor to Acquirer Interface, UK Finance Standard 70.
- Pass a security integrity evaluation process by a PCI Security Standards Council approved testing laboratory (PCI PTS Testing and Approval Programme).
- Payment Card Industry Data Security Standards (PCI DSS) – (This compliance may be provided through the services of a third party provider).
- Payment Card Industry Data Security Standards (PCI PA-DSS).
- Type approval specifications as set by EMVCo (level 1 Electromechanical, level 2 Kernel software).
- The UK Finance Common Criteria Evaluation (EAL4+). Evaluation completed against the **JIL** Terminal Evaluation Methodology Subgroup (JTEMS) POI Protection Profile or;
- Common.SECC certification and registered on the Common.SECC web site.

Payment Transactions

All payment transactions processes must operate in accordance with UK Finance.

All payment transactions processes must operate in accordance with Payment Card Industry Data Security Standards (PCI DSS).

All Payment applications processes must meet Data Security Standard (PA-DSS).

All payment transactions processes must operate in accordance with the Acquirer Bank regulations and standards.

From 2nd April 2016 all card payment surcharges to passengers have been removed. (TPH notice 09/16)

Data Protection

You are legally obliged to comply with the requirements of privacy and data protection legislation in respect of all transaction processes, data management and storage. This includes the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. You can find out more about your obligations from the Information Commissioner's Office (ICO).

Note:-

Sending or handling personal data outside the European Economic Area (EEA) must comply with the specific principle(s) set out in GDPR to ensure an adequate level of protection is in place for the storage and processing of personal data. Compliance

issues may be avoided by ensuring the any cloud data handling is restricted to servers domiciled within UK the countries that make up the EEA.

Documentation Required

- PCI DSS certification (PCI-PTS and PCI PA-DSS where relevant to the solution configuration).
- EMC certification/documentation (where applicable).
- UK Finance Common Criteria Evaluation (EAL4+) certification/documentation, or; Common.SECC certification.
- EMVCo. Type Approval certification/documentation.
- Confirmation of registration on the public register of data controllers maintained by the Information Commissioner's Office (where applicable).

Signage

TfL Signage must be displayed identifying the payment cards/method accepted; these should be placed for view from the exterior and interior of the vehicle as specified by TfL.

The signage must be displayed in such positions so as to minimise obstruction of vision and to make it as visible as possible to passengers after entering the vehicle (Please refer to the document: Guidelines for Advertising on Licensed London Taxis and Signs on Licensed London Private Hire Vehicles.) which can be viewed on the LTPH website www.tfl.gov.uk/tph