Certificate No. C – 00177

ITSO Certificate of Compliance

To: **Unicard Ltd**
Peartree Business Centre, Cobham Road, Ferndown Industrial Estate, Wimborne BH21 7PT

For: **Unicard Remote POST**
Software version: 5.0.1.2;
ITSO console Test Terminal version: 2.1.4.32435;
Housekeeping: 2.1.4.62

This is to certify that the above product has been tested as required by ITSO for compliance against ITSO TS 1000 Specification Version: 2.1.4 Corrigendum 9

Test Report Ref: ***24022017 – Unicard R_POST - P_2.1.4_DR – V.4.0 dated 24 February 2017***

This product supports the functions: ITSO POST and communicates within an ITSO environment as listed in Schedule A of this Certificate.

This product may only be used by ITSO Licensed Members complying with the conditions and constraints listed in Schedule B.

Signed for and on behalf of ITSO: ____________

Title: CHIEF EXECUTIVE OFFICER

Dated : 10 JULY 2017

Certificate Valid until : 9 JULY 2024

Schedule A

The Remote POST kernel covers the same functionality as the Unicard POST kernel but from a server. The Remote POST has a topology with the Customer Media Interface, Business Logic and ISAM all separate.

The architecture of Unicard Remote POST is as follows:

- The POST Server is a Web service hosted by IIS in a Windows server. It consists of locally linked (not separated in communication terms) modules, which are HL2, Housekeeping, Command processor and the application server itself, which exposes the web-interfaces. The SAM and the POST server will be hosted in a secure data centre with access control.
- The Client application(s) could be Web-Browsers or standalone applications and are located on public or private Remote POSTs, i.e. Station Ticket Machines or home, corporate, etc. users. Client applications communicate with the POST Server through a secure public internet connection.
- The Customer Media Interface can be located together and linked locally with the client application, or entirely separated at fixed IP address for example. In case of a local CMI, POST Server interacts with the Customer Media Interface through the Client application, more precisely through the http responses which the Client application receives in return of its requests to the POST Server. In case of separated CMI, the POST server interacts directly with it.

This Remote POST communicates with CMD2, 4 & 7 and uses secure messaging between the customer media and the ISAM. The trust methodology used between the business logic and the Remote Post Server ISAMs is 'Mutual Authentication'.

The IPEs supported are represented by the following table.

IPE	Create	Modify	Accept	Delete
TYP 2 – Stored Travel Rights	✓	✓	✓	✓
TYP 14 – Entitlement	✓	✓	✓	✓
TYP 16 – ITSO ID and Entitlement	✓	✓	✓	✓
TYP 22 – Area based ticket (FR1 and FR2)	✓	✓	✓	✓
TYP 23 – Journey Ticket (FR1 and FR2)	✓	✓	✓	✓
TYP 24 – Journey Ticket With Reservations and Special Restrictions	✓	✓	✓	✓
TYP 27 – Period Pass (space saving)	✓	✓	✓	✓
TYP 29 – Multi Journey Ticket (space saving) (FR1 and FR2)	✓	✓	✓	✓
TYP 29 FR 2 – Multi Journey Ticket (space saving)	✓	✓	✓	✓
Transient Ticket Log (FR1, FR2, FR3 and FR4)	✓	✓	✓	**N/A**

Hot Lists and Action Lists are supported, although Action to take 1: creating IPEs with embodiments are not supported.

Schedule B

This Part 11 solution was tested with a cx21 reader (Orbit-SAMUSB HW version –V2RA; the same as the certified POST kernel reader) and a Gemalto IDbridge K30 ISAM Reader.

Other alternative readers may work acceptably, but are not endorsed by ITSO.

List of the conditions and/or constraints applied by ITSO:

- 0807 messages are not supported by the POST.
- Action to take 1: Creating IPEs with embodiments are not supported.
- Benchmark readings for all the supported CMDs were over the threshold. Note that the benchmarking has been performed to measure the performance of the card validations, although benchmark readings are not applicable for a Remote-POST.