1. Description

1.1 Checkout UI is an off-the-shelf payment page) that enables Customer to collect payments and/or tokenize card data via a payment form.

2. Key features

2.1 This solution is a layer that interfaces with our Payment Platform, allowing Customer certain options to customize the look and feel of the payment page form to align with Customer's branding and look and feel.

2.2 This solution offers a payment form in various languages and currencies, configurable by Customer.

2.3 Customer can accept any card payment or any APM available on our Payment Platform (if Customer has already contracted the relevant solution).

2.4 This solution can be integrated within Customer's website.

2.5 The integration involves a server-to-server call to a Checkout UI REST API, which returns a URL to payment page hosted by us.

2.6 The consumer can be redirected to this payment page on the Customer's website shopping/booking flow to allow payment

2.7 Customer can accept payments as is or through a token generated by our tokenization solutions.

2.8 When using Checkout UI for tokenization, the elements of the payment form containing PCI DSS sensitive data (such as card number and CVV) are hosted by us via an iFrame, allowing Customer to reduce its PCI DSS obligations.

2.9 This solution offers a payment form in a range of different languages and currencies as standard, configurable by the Customer.

2.10 Through Checkout UI, the Customer can accept any card payment or any alternative method of payment available on our Payment Platform, provided that such a method of payment is already contracted by the Customer.

2.11 Also, when used for tokenization, the Customer can tokenize the payment card data (card number and CVV) as part of a payment transaction or as a separate transaction where only the payment card data is tokenized, and no payment is taken.

2.12 This solution can handle transactions in a PNR-integrated (updating the payment transaction and/or a standalone mode.

2.13 This solution helps Customer reduce its PCI DSS compliance obligations.

3. Disclaimers and limitations

3.1 This solution is a web-based solution for online payments and is not a native app like iOS or Android.

3.2 This solution uses the Angular open-source web application framework and the associated Angular material user interface component library.

4. Version control - REST API

4.1 Release versions.

4.1.1 New Releases (v 1.1, v 1.2, etc.) are released when:

(a) a new backwards-compatible feature is released (no breaking changes).

4.1.2 New Versions (v 1, v 2, etc.) are released when:

(a) a new non-backwards-compatible feature is released (breaking change -typically major new feature-);

4.2 Frequency of releases.

4.2.1 Versions for new features are released as new features finish development (no set timeline).

4.2.2 Versions for Angular are done as Angular release new versions (typically every six (6) months).

4.3 Customer updating to new versions.

4.3.1 To ensure PCI DSS compliance, we deprecate all Checkout UI versions using Angular versions where security support has expired.

4.3.2 To leverage a new feature, or the most recent Angular version, Customer must update this solution as soon as this is available and at least once (1) a year to ensure Angular support.

4.4 Support of older versions.

4.4.1 We support the current major version and the previous major version (only bug fixes added to the previous major version) of Checkout UI. We deprecate older major versions.

4.4.2 We support the preceding version of Checkout UI for twelve (12) calendar months.

4.4.3 We will advise Customer of upcoming new versions and release notes that will be published in the solution user guide, including an end-of-support date.

5. Integrations

5.1 Checkout UI must be integrated into a Customer's web application.

5.2 Other integrations with Customer's front and back ends may be available, subject to further scoping.