

First payment solution to support enhanced, secure and contactless payments on common-use platforms

There is a global requirement to ensure airlines use Chip and PIN payment devices to reduce fraud risk. SITA Flex Payments addresses the need for airlines to be able to accept payments securely at airports when using a shared IT infrastructure. The solution enables payment transactions by multiple airlines utilizing multiple DCS's through a shared payment device

BACKGROUND

Touchless is a key requirement

Passengers want touchless, contactless check-in

Non-compliance to card brand rules

Transactions need to be authorized and processed as 'card present'

Non-compliance to EU PSD2 SCA Law.

Without chip and PIN, banks decline to process transactions, or risk being fined.

PIN entry device (PED) required, but not common use (until now)

Off-the-shelf payment terminals are designed and coded to send payments from one merchant to their one bank. They could not be shared, until now.

Increased financial risk

Airlines are liable for fraudulent, counterfeit and charged-back transactions when not using Europay, Mastercard, Visa (EMV/chip) PEDs.

Complex security audit procedures

Airports must ensure the payment system they provide to airlines is capable of compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) requirements.

SOLUTION

- This is the first payment solution allowing airlines to accept payments with enhanced security at airports using a shared IT infrastructure.
- SITA deploys a P2PE based solution to airlines and airports, encrypting card data from point of reading to the bank.
- P2PE technology is combined with EMV and PCI compliant chip card payment terminals, applications and processes. This lets multiple airlines (merchants) use the same terminal while meeting PCI security standards, EU PSD2 SCA and bank requirements.
- The solution includes PCI accredited security mountings, which ensures protection of the endpoint devices and reduces the scope for interference.
- The service can be used at other airports.

BENEFITS

- Contactless
- Single chip-enabled PED enables any airline on any DCS and payment service provider (PSP) to complete transactions
- Enables secure reading and encryption at the payment device which increases data security and reduces the risk of fraud
- Airlines use their PSPs, leveraging existing relationships and combining payment types (i.e., eCommerce) to gain favorable processing fees
- Easier to budget as there are no fees per transaction
- Supports contactless, chip and PIN and magnetic stripe (encrypted) payment options.
- Industry standard PEDs
- Utilizes SITA Data Center which is PCI compliant
- P2PE solution reduces the scope and number of addressable requirements during a PCI DSS assessment

RESULTS

The same security technology used in chip cards to fight counterfeit fraud is also available in **contactless payment cards** which allow users to simply "tap" on the terminal to make a payment."

76% decline

In counterfeit fraud dollars for merchants who completed the upgrade to chip and PIN terminals.

* Decline based upon December 2018 compared to September 2015.

Source: VISA Chip Card Update, May 2019

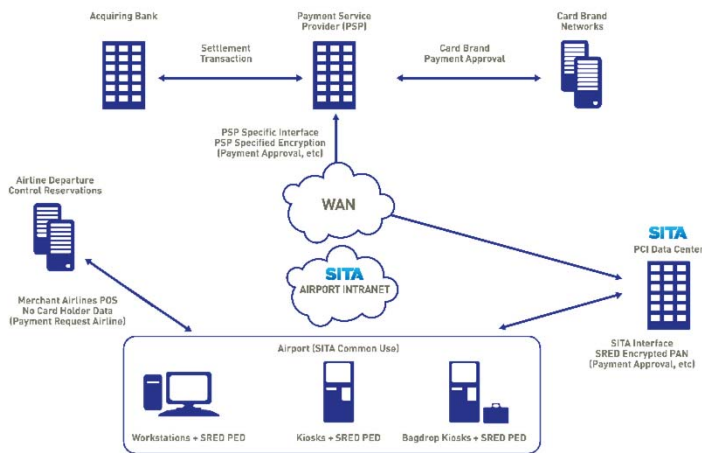


AT AIRPORTS

SITA Flex Payments



How does it work?



- Uses existing CUTE/CUPPS workstations
- Works on CUSS kiosks and self-bag drops
- New peripherals for payment processing
- Gateway on the workstation communicates with PED
- Service infrastructure is hosted in the SITA PCI compliant Data Center



SOLUTION COMPONENTS

1. Payment device - PED

The payment device and software are PCI certified. The device is tamper-resistant and conforms with PCI P2PE requirements.

2. Workstations, kiosks and self-bag drop

Supports the payment device like any other peripheral connected on the platform. The communications between payment device and airline payment application are delivered through the payment gateway developed for this solution.

3. Data encryption

The payment device is deployed with a SITA P2PE key and an online PIN key as part of the service. As per PCI P2PE standards this key is injected to the device prior to shipment from VeriFone. The key injection facility is provided by VeriFone and complies with the PCI P2PE specifications and requirements documented by the PCI council.

4. Message handling and transmission

The payment transactions for a particular airline are transmitted correctly to the airline specified PSP or host. The transaction is translated via the hardware security module (HSM) to the relevant airline key and communicates the payment request to the PSP

CASE STUDY

For the past 8+ years, IATA and the air transport industry have been trying to design a common-use payment service.

There has been a shift in liability for fraudulent transactions to airlines and requirement to comply with the security laws and PCI DSS. The industry is therefore keen to minimize the fraud threat and implement a P2PE compliant payment ecosystem.

The SITA solution uses existing PSP arrangements and processes and provides all required components and technical support.

SITA has successfully deployed the SITA Flex Payment solution, proving the effectiveness of the encryption technology for chip, magnetic stripe and contactless card payment transaction.

For more information please contact us at info@sita.aero