Card Payment acceptance at Common Use positions at airports

Business requirements

Version 1, published in June 2016

Preamble

Common Use (CU) touchpoints (self-service positions such as self-service kiosks or bag drops, and agent positions such as check-in desks, bag drops, gate positions) are increasingly called to perform sales transactions, which requires the acceptance of a payment instrument if the transaction is to be performed end-to-end at the CU position. Card payment is presently the payment instrument of choice for the passengers and for the airlines. However, accepting card payment at CU positions is practiced only by some airlines in some regions, hence it is currently conducted in very disparate ways.

The card industry is progressively rolling out EMV chip cards, which substitute chip to magnetic stripe acceptance. In addition, there is an over-riding demand that card payment acceptance be conducted with strict PCI DSS compliance, in order to safeguard customer's data and merchant's reputation. While some airlines process CU transactions as Card Not Present, the business trend is to move towards Card Present.

Consequently, the industry has been reviewing how card payment acceptance should be conducted at CU positions, and there is an increasing demand for guidance on what are the desirable components of a solution that would support the unique 'multi-merchants/multi-acquirers' business model of CU positions which are shared by several airlines.

The following business requirements stream from the on-going discussions held at industry forums and represent recommendations that airports and/or airlines should consider when drawing up their own business requirements. They do not recommend any technology or provider, and only seek to establish the key components of an effective industry card payment for this specific environment.

Disclaimer: The information contained in this document is subject to constant review in light of changing requirements and regulations. No reader should act on the basis of any such information without referring to applicable laws and regulations and without taking appropriate professional advice. Although every effort has been made to ensure that the information in this document is accurate and current, IATA shall not be held responsible for loss or damage caused by errors, omissions, misprints or misinterpretation of the content hereof. Furthermore, IATA expressly disclaims all and any liability to any person in respect of anything done or omitted, and the consequences of anything done or omitted, by any such person in reliance on the contents hereof.

1. A few definitions

The card industry is in the process of conducting a world-wide technology migration of the ‘face-to-face, card and cardholder present’ sales, moving from magnetic stripe (magstripe) to EMV chip. The following seeks to clarify terms and some of the key business principles that drive the ensuing business requirements for an effective industry card payment solution for CU positions.

1.1. Stakeholders

Because of the complex multi-merchants, multi-acquirers nature of Common Use payments in an airport environment, as many as thirteen different stakeholders could be contracted to deliver services for the overall solution. For the purpose of this document, three categories of stakeholders have been defined below.

Merchant

The ‘merchant of record’ is the entity that is selling the product or service to the cardholder, and collecting the produce of the card sale.

A merchant is contractually responsible vis-à-vis the acquirer for the PCI DSS compliance of the entire transaction lifecycle. When an airline contracts an airport and the airport contracts in turn a vendor to provide card payment services related to CU environment, PCI DSS demands that the roles and responsibilities of each entity in terms of safeguarding sensitive card data be specified.

Acquirer

The acquirer, or acquiring bank, is the financial entity that has entered into a bilateral card acceptance merchant agreement with the merchant (see merchant’s definition) selling products or services to the cardholder. The acquirer is chosen by the merchant. The acquirer is operating under a license, or other form of agreement, from a scheme, which has similar arrangements with the issuer who services the cardholder (see issuer’s definition). For some card brands, the card scheme may also operate as the acquirer and/or issuer, and supports directly the merchant and/or the cardholder.

Issuer

The issuer, or issuing bank, is the financial entity that has entered into a bilateral agreement with the cardholder. The issuer is operating under a license, or other form of agreement, from a card scheme, which has similar arrangements with the acquirer who services the merchant (see acquirer and merchant’s definitions). For some card brands, the card scheme may also operate as the acquirer and/or issuer, and supports directly the merchant and/or the cardholder.

1.2. Further definitions

Card Authentication Method (CAM)

It describes how the card interacts with the card acceptance device, and how it is recognized by the terminal as a valid card.

While the worldwide EMV migration is on-going, cards continue to retain their magnetic strip feature for the time being.

At the time the present document is written, the current EMV Chip specification is EMV 4.3 from November 2011. More information on EMV can be found at http://www.emvco.com/

Cardholder Verification Method (CVM)

A method used to verify whether the person using the card application is the legitimate cardholder. The following CVMs exist:

- No CVM Required
- Signature[1]
- On-line PIN validation: the PIN is encrypted and transported in the authorization request, in order to be verified by the issuer, and the verification result is sent back within the authorization response message.
- Off-line PIN validation: the PIN is verified off-line by the chip.

A chip card may be programmed by the issuer:

- To demand that a PIN validates all purchases, or only purchases above a certain amount. This is referred to as ‘chip and PIN’.
- Not to demand a PIN for any purchase, which is then validated by the signature, as for magstripe-only cards. This is referred to as ‘chip and signature’.

Issuers are free to decide if they want to issue ‘chip and PIN’ or ‘chip and signature’ cards.

In the US, the expression ‘chip and choice’ is commonly used to describe a situation where the issuers are releasing both ‘chip and PIN’ and ‘chip and signature’ cards, which may also be called ‘PIN preferring’ and ‘signature preferring’.

[1] No self-service terminal can support signature-verification as this function can only be performed by a sales attendant.

Chargeback rules

A chargeback is a function initiated by the issuer requesting the acquirer to credit the issuer for the amount in question of a given transaction. Chargeback rules materialize the exact measure of protection (or left over risk) that the merchant bears. Rules can be defined at:

- National level (where both the card and the place of transaction are from the same country)
- Intra regional level (where the card and the place of transaction are from two different countries belonging both to the same region)
- Inter regional level (the card and the place of transaction are from two different countries belonging to two different regions)

As a consequence, the protection the merchant has against fraud chargebacks may differ depending on the geographic location of the transaction.

It is up to each merchant to analyse with its acquirers the exact chargeback rules applying to his business, per card brand and per country of origin of the card.

(Fraud) liability shift

Under the terms of the merchant agreement, a merchant attains some level of protection against the consequences of fraud (i.e. the fraud chargebacks) depending on the capability of the card acceptance device.

As a rule, the merchant deploying the highest capability for secure card payment acceptance attains the highest level of protection, <u>even if</u> the card or the issuer do not match that highest level of security.

As an example, a ‘chip and PIN’ terminal will usually protect the merchant against any fraud that can be perpetrated against a magstripe-only credit card, as the card has no chip (to prevent Counterfeit fraud) and does not support PIN validation for purchase (to prevent Lost and Stolen fraud).

The fraud liability shift principles are translated into the chargeback rules of each card scheme, which define the exact measure of protection, or left over risk that the merchant bears.

PCI DSS compliance

The Payment Card Industry Data Security Standard (PCI DSS) is composed of the joint set of technical requirements of American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. data security compliance programs. The international card schemes each enforce compliance with the standards in their respective network.

Card payment sales conducted at CU positions fall in the scope of each airline's own PCI DSS obligations, though they are conducted at 'shared airport infrastructure' (CU position, airport network) which are not under the direct control of a single airline.

There is no PCI DSS certification for a payment acceptance terminal, as PCI DSS compliance is evaluated for the complete end-to-end transaction environment, from the customer-facing device to the card remittance file delivered to the acquirer.

However, a Payment Application certification process called PA-DSS helps the software vendor to develop payment applications that will help the merchant in obtaining a PCI-DSS certification for its end-to-end card transaction environment.

At the time the present document is written, the current PCI DSS specification is PCI DSS v3.2 from April 2016. More information can be found at:
https://www.pcisecuritystandards.org/document_library

Self-service terminals

Self-Service unattended acceptance terminals[2] exist in many retail sectors and designate an unattended Point Of Sale (POS) System (e.g. vending machine, check-out kiosk) where the cardholder conducts the transaction at the Point Of Interaction without the participation of an attendant, and where some security verifications cannot be performed (such as if the card appears to be genuine, or if the signature matches the one on the panel on the back of the card).

Terminal Type Approval

Type Approval is a process that a product or solution must undergo in order to obtain the authorization for deployment from a given card payment scheme or Approval Body. EMV Co Type Approval testing is divided into two levels:

- The Level 1 Type Approval process tests compliance with the electromechanical characteristics (contact) or the analog characteristics (contactless) and logical protocol requirements defined in the EMV Specifications.
- The Level 2 Type Approval process tests compliance with the application requirements as defined in the EMV Specifications.

[2] Depending on the card schemes, self-service/unattended acceptance terminals could be referred to as Customer Activated Terminals (CAT) or Self-Service Terminals (SST).

2. Scope of the business requirements for CU positions

Both self-service and agent positions are in scope.

During the meeting in September 2015 of the Passenger Experience Management Group (PEMG) 13, it was agreed that there was no immediate need to take payments at a CU self-service bag drop because of the long processing time and resulting queues[3].

3. Business requirements for CU positions

The airlines have defined the following business requirements for self-service and for agent positions, in order to assist both airlines and airports in searching for alignment on solutions that can be implemented globally, thus easing the investment and roll out burden on all stakeholders.

		Self-service position	**Agent position**
The solution must enable the merchant to achieve and maintain PCI DSS Compliance		Must have	Must have
Transaction type	**Ticket sale**	Nice to have	Must have
	Ancillary sale	Must have	Must have
Card payment brand	**Visa**	Must have	Must have
	MasterCard	Must have	Must have
	American Express	Must have	Must have
	Other card brands	As per the appreciation of the group of airline users of the CU position	As per the appreciation of the group of airline users of the CU position
Card Authentication Method (CAM)	**Magnetic stripe[4]**	Must have	Must have
	EMV chip	Must have	Must have

[3] This can be reviewed at a later date.

[4] The categorization is 'Must have' for both self-service and agent positions in order to support the current environment.

		Self-service position	Agent position
100% on line authorization for magstripe transactions		Must have	Must have
Certification	EMV Co Level 1 type approval	Must have	Must have
	EMV Co Level 2 type approval	Must have	Must have
	PA DSS v3.1	Nice to have	Nice to have
Contactless[5]	Capable	Must have	Must have
	Enabled	Must have	Must have
Cardholder Validation Method (CVM)	No CVM	Must have	Must have
	Signature		Must have
	On line PIN	Must have	Must have
	Off line PIN	Must have	Must have
No airline merchant dependency on a single payment provider (processor or acquirer)		Must have	Must have
Number of supported merchant airlines		Must fit the number of airlines sharing a CU position	Must fit the number of airlines sharing a CU position
Must be capable of supporting multiple merchants of record		Must have	Must have
Card retention capability		Not required	
Provision of a receipt[6]		Highly recommended	Highly recommended

For any comments or questions, please contact: pci@iata.org.

[5] MasterCard Global Operations Bulletin 11, 3rd Nov 2014, demands that as of Jan 1st 2016, all newly installed terminals with contactless capability be contactless-enabled. Visa Europe has the same mandate as MasterCard Europe, according to 'Payment Cards and Mobile' (10 12 2015).

[6] Subject to eventual local requirements that a paper receipt be provided.